Guideline - CRISIS RESPONSE PLANNING MANUAL (CRPM) - Part 3 / Volume 2

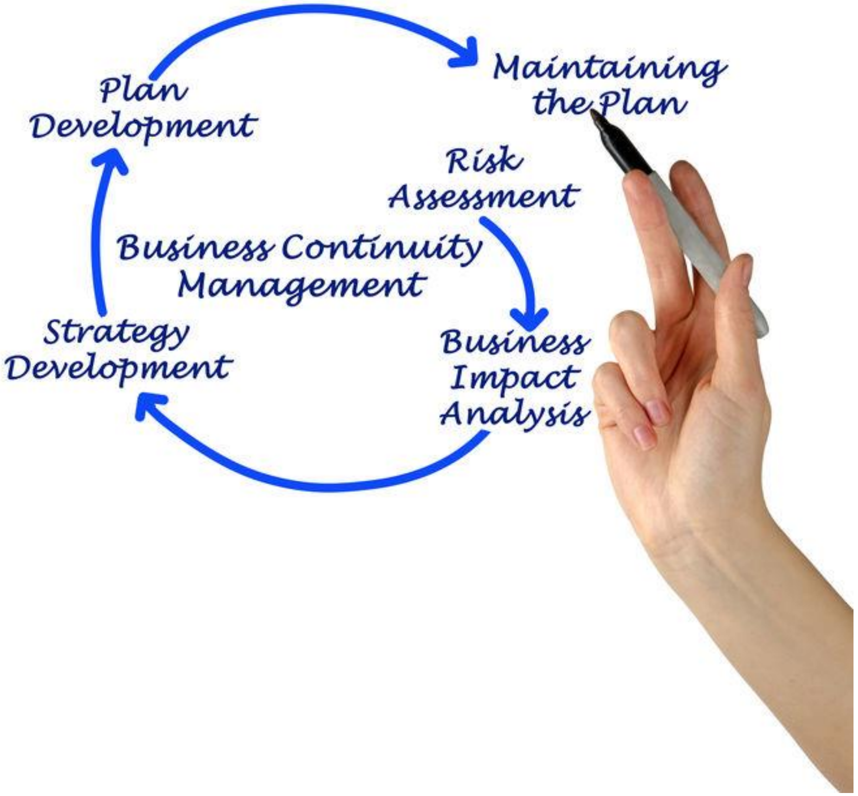
Business Continuity Management - in an Aviation Context

Putting it all Together - The 'Detail'

Example: Extract from the 'Vikings' Business Continuity Plan - Circa 810 AD / CE

Key Product:	Raid & Pillage
Critical Resource 1:	Longboat Sail(s)
Threat:	No Wind
Risk:	High
Probability:	Medium
Impact:	Unacceptable Business Loss
BC Strategy:	Find other Means of Propulsion
BC 'Tactical Solution':	Use ~~Whores~~ Oars
MTPD (MAO) / RTO:	Zero / Immediate
MBCO:	Full Recovery (100% Ready to Raid)
Support Resource 1:	Manpower
Support Resource 2:	Oars
Support Resource 3:	Whips
Support Resource 4:	Luck!

ACT
PLAN
DO
CHECK


Plan Development
Maintaining the Plan
Risk Assessment
Business Continuity Management
Strategy Development
Business Impact Analysis

Analysis
Plan
Assessment
Process
RISK
Management
Control
Check
Strategy

BIA
Business Impact Analysis

STRATEGY

+

SOLUTIONS

BCP

TRAINING

Biz Infographic
Lorem ipsum dolor sit amet consec
tetur adipisicing elit sed do eiusmod.
01
Biz Infographic
Lorem ipsum dolor sit amet consec
tetur adipisicing elit sed do eiusmod.
02
Biz Infographic
Lorem ipsum dolor sit amet consec
tetur adipisicing elit sed do eiusmod.
04

EXERCISING

MAINTENANCE

EVALUATE
EXAMINE
ASSESS
MEASURE
REVIEW

Deliberately Blank

Revision Information

This CRPM Part 3 / ***Volume 2*** document comprises 319 pages - all dated 10 June 2021

Revision No	Date	By
* Revision (Original)	30 Jul 2010	A H Williams (author / owner)
** Revision 1	01 Oct 2012	A H Williams
** Revision 2	01 Sep 2014	A H Williams
** Revision 3	01 May 2016	A H Williams
** Revision 4	01 March 2017	A H Williams
** Revision 5	01 March 2018	A H Williams
** Revision 6	01 May 2019	A H Williams
*** Revision 7	10 March 2020	A H Williams
Revision 8	10 June 2020	A H Williams
Revision 8A	10 June 2021	A H Williams

* Based generally on **BS 25999** (ISO 22301 / ISO 22313 formally superseded BS25999 on 01 June 2014)

** Guided ***to a degree*** by **ISOs 22301:2012** & **ISO 22313:2012**

*** Up to early 2020 the contents of this document (CRPM Part 3 / Volume 1) formed part of what was then a ***single*** document of more than ***300*** pages - entitled simply ***CRPM Part 3***

With the issue of ISO 22301:2019 and 22313:2020 around late ***2019*** / early ***2020*** respectively - the author owner of the CRPM Part 3 document decided to ***split*** the latter into **two**, ***separate*** volumes

Volume 1 (separate document) covers general, introductory and background material - whilst ***Volume 2*** (you are reading it right now) provides the associated 'detail'

This document shall be reviewed and revised by its author / owner on an 'as required' basis - being at least 6 monthly. Should a review result in the need for a revision - the latter shall be actioned and the associated controlled document information updated accordingly. Note that each time that a revision is incorporated - the ***entire*** document will be re-issued electronically - with the revision already having been incorporated by the author / owner

The current (latest revision included) version of ***this*** document can always be found at:

https://www.aviationemergencyresponseplan.com/guideline-template/

'CRPM **Part 3** / **Vol 2** - **Intro** to **Aviation Related Business Continuity Planning**'

Any hard copies made of this document should be regarded as uncontrolled - unless the entity / person so doing has taken appropriate action to ensure that the hard copy may be regarded as 'controlled' - within their own sphere of operation - whatever that might be

Control of Documented Information

See pages 58 and 113 - ***before*** starting any tasks/work associated with CRPM Part 3 in general

Preamble

This guideline document (CRPM Part 3 / ***Volume 2)*** follows on from the introductory info provided in (separate document) CRPM Part 3 / ***Volume 1***

It is suggested that the reader does not try to utilise / apply the information contained herein without firstly having acquired a reasonable working knowledge of what is contained in Volume 1. That this has been achieved is now used as the basis for what follows in this Vol 2

Unless indicated otherwise in ***this*** Vol 2, all of the introductory info from Vol 1 can be assumed to also apply (in this Vol 2) - and is thus not repeated

Contents

The original CRPM Part 3 (written in 2012) was a ***single*** document until late 2019 - when it was split into two separate volumes (you are reading ***Volume 2*** right now). The original Section 1 of the '***old***' CRPM Part 3 contained introductory and explanatory material. This latter has been moved to the 'new' Volume 1 ***only*** - as part of the split (i.e. not included in this Vol 2)

Accordingly (and to save a lot of 'readjustment' time, work and and) a 'Section 1' is still retained '*notionally*' in this Vol 2 - but there is nothing in it i.e. everything starts in ***Section 2*** - page 19

Note - Section 5/2 mainly relates to 'Business Impact Analysis' and 'Risk Assessment' (i.e. 'understanding the organisation' type / related activities)

IMPORTANT: See boxed note at bottom of page 45 - and then return here

Acronyms / Abbreviations etc

BC	Business Continuity
BCPM	BC Programme Management
BCMS	BC Management System
BCP	Business Continuity Plan
BCT	Business Continuity Team
BIA	Business Impact Analysis & Solutions
BRP	Business Recovery Plan
BRT	Business Recovery Team
CIQ	Customs, Immigration & Quarantine (Port Health) Services (aviation related)
DMC	Disruption Management Centre
DSU	Disruption Support Unit (see also IBU)
ERP	Emergency (Crisis / Incident) Response Plan
ERT	Emergency (Crisis / Incident) Response Team
GHA	Ground Handling Agent (Airline Representative)
IBU	Individual Business Unit (part of a larger entity) (see also DSU)
ICAO	International Civil Aviation Organisation (A body of the 'United Nations')
ICT	Information and Communications Technology
IRS	Incident Response Structure
ISO	International Organisation for Standardisation
MAO	Maximum Acceptable Outage (i.e. a period of time) (see also MTPD)
MBCO	Minimum Business Continuity Objective (i.e. an operationally related level of continuity - as related to provision of product, services etc. in a 'disruption' type context)
MMS	Modern Management System
MRO	(Aircraft) Maintenance, Repair and Overhaul Organisation
MTDL	Maximum Tolerable Data Loss (relating specifically to ***data*** & ***documentation***)
MTPD	Maximum Tolerable Period (i.e. a time) of Disruption (re a related product, service, activity etc.) (See also MAO)
RA	Risk Assessment
RCA	Resources Consolidation Analysis
RM	Risk Management
RPO (CDP)	Recovery Point Objective (Critical Data Point relates to ***data*** & ***documentation***)
RTO	Recovery Time Objective
SMS	Safety Management System
SPOF	Single Point of Failure
TM	Top Manager (organisation's most senior executive) /Top Management

Deliberately Blank

Section 1 / **’NOTIONAL SECTION ONLY’**

Deliberately Blank

IMPORTANT NOTE

THE SECTION *NUMBERING* SYSTEM USED THROUGHOUT *THIS* CRPM PART 3 / VOLUME 2 DOES *NOT* RELATE DIRECTLY TO THE EQUIVALENT NUMBERING (Clause) **SYSTEM(s) USED IN** (Separate Documents) **ISOs 22301 and 22313**

Section 2 / INTRODUCTION

Evolution of BC

The concept and practise of * business continuity (BC) is both relatively new (say from about the 1970s onwards) and something dating back to the beginning of mankind

* Pedantically speaking we should be using the term '***Risk Management***' here - as BC is simply a component part (amongst others) of the latter

Taking the last point first - humans have always devised alternate methods of accomplishing important tasks (which get disrupted), typically as a matter of necessity - or even survival

For example, early hunters / gatherers (in order to take care of the possibility that what was being hunted / gathered might not be available [temporarily or permanently - for whatever reason]) eventually 'discovered' farming. The latter, in turn, lead to a 'need' for irrigation outside of any rainy season e.g. by use of wells, dams, irrigation systems etc.

Another example refers to some early, sail powered boats having a backup propulsion system to account for times when the wind did not blow / did not blow in the desired direction i.e. use of oars + humans to 'operate' them

However, only in the recent past (say from about the mid-1980s onwards) has BC become to be regarded 'by some' (rightly or wrongly) as a professional discipline in its own right - similar to quality, risk and security etc. management

The origins of ***modern*** BC lie in:

- Risk Management
- Traditional *emergency / crisis / contingency* response management
- (ICT etc. related) 'disaster recovery' .... and something known generically today as:
- 'Societal Security'

Relatively recent emphasis on 'Corporate Governance' (Governance, Risk & Compliance - GRC) has also placed more focus on the importance of BC (whatever might be the nature of the organisation which is subject to the corporate governance)

It is important to note that BC does not replace other, associated disciplines (emergency / crisis response; risk management; ICT related disaster recovery etc.) - but is accomplished ***in conjunction with them*** - where appropriate (in fact and pedantically speaking [and as already mentioned], ***BC is simply a subordinate component of risk management***)

BC has also become increasingly high profile given the turbulent '***global environments***' in which we now live - ranging at the 'more impacting' levels from natural disaster, cyber vulnerabilities, global economic recession, pandemic illness, major international crime, terrorism etc. ....to the more mundane but still potentially serious occurrences e.g. fire, flood, sickness, industrial action, denied access to facilities & information, information loss etc.

The potentially ***adverse*** impacts of such global environments on an organisation's plans, services, products, activities, manpower, profitability, reputation, brand, image etc. - can be considerable and, if they actually do impact, could lead to * '***unacceptable***' consequences - and even failure (of the involved organisation[s]) in extremis

* Note - the meaning of '***unacceptable***' is typically defined / decided by the organisation itself

Effective, efficient and timely BC intervention can assist in adverse impact reduction (mitigation) of (and timely recovery from) such unacceptable consequences. As such, BC can thus be an asset to ***any*** organisation - and whilst it (BC) might be intangible, like any asset it has worth / value

** Establishment of good BC practices (typically via introduction of a 'business continuity management system' - BCMS) ***by an organisation*** not only assists in protecting it from potential damage / failure - but can also contribute to the 'bottom line' e.g.

- Contributes to overall resilience in general
- Contributes to the identification and addressing of operational vulnerabilities
- Can assist in protecting life, assets, the environment etc.
- Can assist in protecting / enhancing reputation, credibility etc.
- Can assist in increasing competitive advantage and mitigating disruption related costs
- Can increase the confidence of stakeholders / interested parties
- Can assist in reducing legal, financial etc. exposure
- Might lead to lower insurance premiums; wider insurance cover for same price etc.
- Might increase profits e.g. due increased customer confidence / satisfaction etc.
- Might attract new customers / clients and retain existing customers / clients
- Potentially increases share price e.g. after successful handling of a major disruption
- Potentially gain 'preferred supplier' status (as appropriate)
- Take advantage of / better manage 'risk' (risk appetite) - if appropriate etc.

** For additional info re the above see also pages 40 and 41

It is important to understand that BC is not necessarily a 'voluntary' concept, i.e. at the whim of organisations as to whether they adopt it or otherwise e.g. see boxed case study on page 63

Business Continuity at its Simplest

We have already seen that 'Business Continuity' etc. (in the wider sense) has been around for a very long time and, even today - basic BC ***can*** still be a relatively simple concept to understand and apply to some areas / types of business, commerce and public sector equivalents

However, the modern evolution of BC into what some now (mistakenly?) see as a professional discipline in its own right, has definitely made the subject more complex and ambitious - arguably unnecessarily so - ***except perhaps*** for its application to the largest of multi-layered and / or multi- disciplined and / or more complex organisations

Indeed, for the vast majority of smaller and medium sized organisations - and some of the ‘simpler’ larger organisations too, modern BC is a reasonably straightforward matter to effectively and efficiently apply - without the need for many of the associated complexities referred to above

It is thus vital that modern BC retains as much ‘simplicity’ as possible, as over-complexity can lead to increased and unnecessary costs, a definite lack of interest in the subject (often by those needing ‘to have such interest’ the most) and an undesirable / undeserved air of ‘mystique’ - which further reinforces the lack of interest factor. This is unfortunate as it can lead to many organisations - capable of fairly easily and relatively cheaply introducing ***simple*** BC measures into their products, services, operations etc. - choosing not to do so

However, we ***do*** need to go considerably further into the more complex aspects of BC in ***this*** Volume 2 guideline - in order that the appropriate user / reader might be more adequately prepared for further training and experience requirements (as appropriate) - typically as related to the ‘professional’ application of BC within an associated organisation such as an airline, an airport, a GHA etc. (many of which are multi-layered, using multiple disciplines in a complex environment)

The term ‘appropriate reader / user’ might typically relate here to those having appointments / positions e.g. as both the Flight Safety Manager ***and*** the Business Continuity Manager for an airline; being both the Quality Manager ***and*** Business Continuity Manager at an airport; e.g. (and, if [rarely] your airline / airport etc. can afford and / or desires it enough) - being appointed ***sole*** Business Continuity Manager with no other role sharing accountabilities

But, for the moment, let’s see how ***relatively*** simple BC can be by looking at the basic steps (pages 28 - 38) required to introduce and implement a typical, (reasonably) simple BC system / programme into an ‘average’ small to medium sized ‘generic’ organisation

Where necessary, refer to the ‘abbreviations / acronyms’ (page 16) and ‘glossary’ (found in *separate* document ‘CRPM Part 3 / Volume 1’)

Should you become frustrated at the ‘complexity’ of BC as you read further in this Volume 2 guideline - just return here from time to time to get a check on reality and perspective!

IMPORTANT

To fully understand the implications of what follows in ‘***Steps 1 and 2***’ (starts page 28) you need to read and understand the following definitions (***reproduced*** [pages 22 - 27 below] from ***separate*** document CRPM Part 3 / Volume **1**)

For definitions of ***other*** terminology used e.g. *Minimum Business Continuity Objective* (MBCO); *Recovery Time Objective* (RTO); *Business Impact Analysis* (BIA); *Risk Assessment* (RA) etc. - see the glossary contained in the above mentioned (separate) document itself

- **Activity**

Processes undertaken by an organisation (and / or on its behalf) which are necessary to deliver and / or otherwise support (directly and / or indirectly) said organisation's individual and / or combined '**KEY product**(s) / **services** / **operations** / **tasks**' etc.

Key ***main*** activities are those whose failure might ***most quickly*** 'threaten' the viability of the associated (parent) ***key*** product(s), service(s) etc.

In an aviation context, they (key main activities) are typically carried out by e.g. ICT services; call / contact (reservations & customer services) centres; operations control centres; fuelling facilities; flight crew & cabin crew services; airport baggage systems; airport / airline freight systems; air traffic services; airport fire and rescue services; terminal and ground handling services; aircraft & airport engineering services; safety and security services etc.

Key ***supporting*** activities are those whose failure might threaten (in varying [generally 'less-urgent]' timescales) the associated (parent) key main activity / activities. In aviation again, key supporting activities typically include in-flight catering; HR, finance, legal & insurance services; facilities & procurement services; medical services etc.

'Activities' (and thus the organisation's departments / business units etc. which carry them out) generally 'do what they do' via implementation of associated **processes**

A particular process can extend (end [input] to end [output]) across several departments / business units - and can be internal and / or external to the organisation e.g. the aircraft refuelling ***process***; the aircraft parking ***process***; the airport check-in ***process*** etc.

Processes are often inter-dependent with / on other processes. They also require the '***support***' provided by ***resources*** (particularly people) in order to function

Activities are typically provided as a mix of those conducted directly by an organisation itself (e.g. airlines and airports) - and those depending on independent, third party suppliers / providers (e.g. ground handlers; fuelling services; CIQ; call centres etc.)

An organisation's activities (+ everything that they depend on as per above) provide the major ***inputs*** for the 2 fundamental aspects of facilitating the management of business continuity i.e.

- **'Risk Assessment'** *and*
- **'Business Impact Analysis'**

……………………………otherwise ***collectively*** known in common use BC terminology as gaining an

'UNDERSTANDING of the ORGANISATION'

- **Key Product / Service / Operation / Task** etc. (See also definition of *'Activity'*)

  What an organisation is primarily all about i.e. what it 'does'

  For example and for an **aircraft** operator - key services / operations might include the transport of passengers by air; the transport of cargo and similar by air; the provision of associated leisure services (vacations, hotel & car hire bookings etc.); provision of search & rescue services by air; fire-fighting operations by air……….. and so on

  For an **airport** operator - key services / operations might include providing passenger and cargo services to aircraft operators; provision of air traffic control services; provision of fire-fighting and rescue services; provision of refuelling services: provision of 'duty-free services etc.

  Significant disruption to an organisation's key product / services / operations etc. – which lasts for a ***significant*** time / period / duration, might have unacceptable (adverse) impacts on the organisation and / or its stakeholders / other interested parties

  Note 1 - the term '***significant***' should be defined by the organisation - as it will typically vary for different types of product / service / operation

  Note 2 - in addition to appearing anywhere else, 'key product / services / operations' should also be documented within the ***'scope'*** section of an organisation's '**BC Policy**' statement

  Note 3 - see also definition of 'product / service'

- **Process**

  An inter-related / inter-active operation - which uses ***resources*** (one or more of which will probably be a procedure) to transform ***inputs*** into ***outputs***. (Note - it is possible that the output from one process can become the input for another. Note also [simplistically speaking] that an organisation's departments / business units etc. typically use associated processes to perform their activities)

  One should be able to ask the following typical questions (and get appropriate replies) when defining a typical 'work' related **process**:

  'Activities' - **What** are the basic jobs carried out in your department / business unit?

  'Inputs / Resources' - **What** inputs / resources do you need to do your work / jobs?

  Where does 'what you need (to have) in order to do your work / jobs' - come from?

  Procedure - Can you explain (in reasonable detail) **how** your 'work / job operations' function?

  'Outputs' - **what** 'deliverables' result from your work / jobs?

Who receives the 'results' (deliverables) of your work / jobs?

How do you know if you've 'done your work / jobs correctly, accurately, on time etc.'?

For a simplistic example of a **process** - take 'making a cake'

The ***input*** comprises the cake ingredients; the ***output*** is the cake and the 'bit in the middle' uses ***resources*** such as the chef / cook, a recipe, utensils, crockery, a stove etc. - to transform the input into the output

Note - in this simple example the ***recipe*** would technically be termed a '***PROCEDURE***' - and what the chef does as **'Key Main Activities'**. There are no **'Key Supporting Activities'** in this particular process

Taking this example a little further - if the cake making process was a part of a 'cake-selling' outlet (e.g. the '***organisation'*** is a cake shop) - then 'cake making and selling' may be considered to be the '**KEY PRODUCT / SERVICE** etc.' of that organisation

Procedure

A ***procedure*** (written or otherwise) is a specific way of carrying out an associated / parent '***process***' - typically comprising (at its simplest and in relation to the latter:

- Who performs what action(s)
- In what sequence the action(s) (+ the defined steps in the action[s]) occur(s)
- The criteria (standard[s]) which must be met in performing the action(s)

Documented procedures can be general, detailed or anywhere in between. Whilst a simple procedure might comprise e.g. just a simple flow diagram, a detailed procedure could be e.g. a one page form or it could be several pages (or many more) of text / flow and other diagrams / images etc.

A procedure typically:

- Defines and controls its ***associated*** (parent) ***process***
- Explains how the above should be accomplished, who should do it, under what circumstances, when / how often etc.
- States and reflects associated authorities, responsibilities, resources etc. - to be assigned / allocated / used
- States which inputs should be used and what outputs should be delivered

- **Maximum Tolerable Period of Disruption** (MTPD) (Maximum Acceptable Outage - **MAO**)

(See also definitions of *'**Activity**'*, *'**Recovery Time Objective** - [RTO]'* & *'**Minimum Business Continuity Objectives** - [MBCO]'*)

Estimated period of ***time*** it would take for the consequences of an adverse impact(s), arising as a result (for whatever reason - but typically termed 'disruption / interruption') of **not** providing an organisation's **key** product(s) / service(s) / operation(s) / activities etc. - **to become unacceptable** to the organisation's (impacted) stakeholders / other interested parties

Overarching (strategic) MTPDs should be estimated, approved & documented for **EACH** of an organisation's **key** product(s) / service(s) / operation(s) / activity(ies) etc. -

……………….followed by MTPD estimations for **each** associated (***subordinate***) key **main** activity etc. required to produce / operate etc. its (parent) key product / service / operation / activity etc. (as required)

Note - The estimation & allocation of MTPDs for ***key main activities*** **may**, in turn, require ***re-adjustment*** of the ***initially*** estimated ***strategic*** MTPDs referred to above

Further MTPDs should then be set, in turn, for **each** associated (***subordinate***) key **supporting** activity required to support its (parent) key **main** activity etc.

Note - The estimation & allocation of MTPDs for key **supporting** activities **may**, in turn, require ***re-adjustment*** of the ***initially*** estimated **key main activity** MTPDs referred to above

Many activities are dependent on the continued operation of external suppliers and similar. Accordingly, the organisation should make all reasonable effort to ensure that suppliers are not / do not become '**single points of failure**'

This can be achieved e.g.

- by use of appropriate 'service level agreements - SLA' within contracts
- by engaging more than one supplier to provide the same product / service
- by requesting suppliers to adopt their own BC measures / techniques - including the setting of MTPDs, RTOs, MBCOs etc. for their own key products, services, operations and activities

IMPORTANT

'***Subordinate***' MTPDs must be ***equal to or shorter*** (in terms of time period) ***than an associated***, '***parent***' ***MTPD***. This is why changes to a subordinate MTPD must then (always) be cross-checked with its parent MTPD - to see if a consequential / associated / knock-on change in the latter is then required……………..and so on

Note 1 - Most (if not all) ‘activities’ comprise a series of associated (subordinate) ***processes***. For the sake of brevity the latter have been ignored in what has been written above (previous page)

However, in reality, all such processes (as associated with their ‘parent’ activities) **must be similarly accounted for** - and any which are considered ‘significant’ from the business continuity viewpoint are to be assigned MTPDs in their own right. Such MTPDs must then be ‘managed’ if necessary - in a similar way to that documented on the previous page

Note 2 - Some typical ‘consideration’ factors used in estimating MTPDs include:

- Potential (adverse) ***impact****(s)* on staff / public well-being (humanitarian; welfare etc.)
- Potential (adverse) ***impact****(s)* re breaches of statutory and / or regulatory and / or ‘best practice’ (including any adopted standards) and / or similar requirements
- Potential ***damage*** to brand / image / reputation
- Potential financial ***damage***
- Potential ***deterioration*** of product / operational capabilities / service quality etc.
- Potential environmental ***damage***
- ***Other*** potential factors specific to / specified by the organisation

Note 3 - The term / words ‘Maximum Tolerable Period of Disruption - MTPD’ might be difficult to correlate with its / their actual meaning, as given on the previous page - and significant debate has occurred (over recent years) concerning same

Such debate is beyond the scope of this guideline document - but suffice it to say that the alternative term ‘**Maximum Acceptable Outage** - **MAO**’ is much preferred by the author / owner of this CRPM guideline document and can be used interchangeably herein

The definition of MAO ***is the same*** as that for MTPD

- **Critically Time-sensitive & Critical Activities** + **associated Resources** & **Dependencies**

  Component ***activities*** (+ their associated processes, procedures, resources, dependencies, inter-dependencies etc.) of a specified key product / service / operation etc. - which, if interrupted for a long enough ***duration*** (significant ***time*** / ***period***), might cause the associated organisation to incur unacceptably adverse economic / operational / reputational etc. impacts

IMPORTANT NOTE - the term '***critical***' *(other similar terms used in BC =* '***essential***', '***high importance***', '***urgent***' *etc.)* as used herein - is typically used in the context of '***TIME***-criticality' - as per the two definitions immediately above

However, it should ***also*** be interpreted (where appropriate) in a ***different context*** i.e. being critical for the purposes of prevention of death and / or injury + similar type impact event / situation - where ***time*** might ***not*** be the ***most*** significant factor. In such case (and for the purposes of differentiation) the term, 'critically time sensitive' might be replaced with the term 'critical'

Step 1

- Identify & document the organisation's ***key*** * *product(s) / services / operations* - followed by estimation, agreement and assignment of an *initial* ***Maximum Tolerable Period of Disruption*** (MTPD) to ***EACH*** - based on the organisation's strategic (overarching / longer term) business objectives and (if applicable / desirable) risk appetite

* For example and for an ***aircraft*** operator - ***key services / operations*** might include:

- The transport of passengers using air operations
- The transport of cargo using air operations
- The provision of associated leisure services (vacations, hotel & car hire bookings etc.)
- The provision of search & rescue services by air
- The provision of fire-fighting services by air
- The provision of air ambulance services ………… and so on

For example and for an ***airport*** operator - ***key services / operations*** might include:

- Providing passenger and cargo related services to aircraft operators
- Provision of 'duty-free' and other airport based retail outlets etc.

Contributing to each identified ***key*** product / service / operation - will be a host of associated (subordinate) ***key main activities*** (processes, dependencies, procedures, resources etc. - some independent and some inter-dependent; some internal and some external)

Examples of the latter for ***aircraft*** operators include:

- Provision of aircraft
- Provision of operating crew
- Network operations services e.g. operational control, flight despatch, flight-watch, crew control, rostering etc.
- Reservations and customer services
- In-flight catering services
- Aircraft maintenance / engineering services
- Fuelling services
- Ground handling services
- Frequent Flier services
- Safety & Security etc.

Note: There are often 'overlaps' in who provides some of the key ***main*** activities listed above e.g. a designated (and typically independent) 'ground handling agent / operator' (**GHA**) might be contracted to provide some of such services on behalf of an associated aircraft operator

Examples for ***airport*** operators include:

- Air Traffic Services
- Ground engineering Services
- Ramp & passenger terminal services

- Passenger departure and arrival operations
- Baggage handling
- ‘Airside’ ground transport services
- Fire and rescue services
- Customs, Immigration and Quarantine (Port Health) services
- Medical services (flight operations related)
- Safety & Security etc.

Many *key main activities* rely, ***in turn***, on a number of associated ***key supporting activities*** e.g.

- HR services
- ICT services
- Financial, legal & insurance services
- Airport car parks
- ‘Groundside’ transportation services
- Commercial / Marketing / Sales services
- Customer services (incl. call / contact centres)
- Procurement & logistics services
- Corporate Communications / PR / Media Relations etc.
- Recruitment and retention
- Training
- Staff / Business Travel etc.
- Medical Services (non-flight operations related) etc.

All such ***activities*** mentioned in this ‘step 1’ typically depend, in turn, on associated (subordinate) ***processes***. The latter depend, in turn, on associated (subordinate) ***procedures***, the provision of required ***resources*** etc.

Step 2a

- For ***each*** ***key*** *product* / service / operation specified in step 1, identify & document (in turn) ***each*** and every associated key ***main*** activity

  For ***each*** key ***main*** activity identified immediately above, identify & document (in turn) ***each*** and every associated key ***supporting*** activity

  Also deal similarly (for each ‘key supporting activity’) with any associated, supporting ***processes***

  Also deal similarly (for each ‘supporting process’) with any associated, supporting ***procedures***

- For ***each*** of the above, differentiate and document / list (in turn, with reasons and in order of an ‘urgency / importance’ related priority to the organisation) those considered by the organisation to be ***critical*** and / or ***critically*** time-sensitive (i.e. the words ‘*critical*’/ ‘*critically*’ being used here in a BC related context - as per definition on page 27)

Step 2b

- Repeat step *2a* (create a ***separate*** list) for all other key ***main*** and key ***supporting*** activities - considered to be ***NON-critical*** and / or ***NOT critically*** time-sensitive (i.e. the words '*non / not critical*' being used here in a BC related context)

Also include any **supporting *processes***, ***procedures*** etc. which might require similar consideration as that documented in step 2a

Step 3

- For ***EACH*** (i.e. one by one) identified ***critical*** and / or ***critically time-sensitive*** activity found in Step *2a* - conduct an ***analysis*** aimed at understanding and then documenting the likely, *adverse* **IMPACTs** on the organisation - should operation of such activity be ***disrupted*** (for whatever reason) for a * ***significant*** period of time e.g. (at its very simplest) classify in terms of high, medium or low adverse impact

* The meaning / context of 'significant period of time' should be decided & documented by the organisation itself

- For ***each*** activity (as per the para above) - ***list*** these adverse impacts in ***descending*** order of 'severity' on the organisation i.e. the most severe being at the top of each list etc. Where adverse impacts are judged to be similar for a particular activity - the organisation's top management should decide their relative position on this list

Note 1 - Steps 1 to 3 above (taken together) are known as '***Business Impact Analysis** - **BIA***'

Note 2 - At this point, associated ***MTPDs***, ***RTOs*** & ***MBCOs*** would then be estimated, agreed & assigned i.e. as applicable to each of the ***critical** and / or **critically time-sensitive*** activities obtained via Steps 2a and 3 above - after firstly accounting for the '***initial'*** MTPDs assigned in Step 1. For the sake of clarity, this has ***not*** been done in this simplified example

Note 3 - MTPDs for key ***supporting*** activities should be equal to or less than the MTPDs set for the ***associated*** (parent) key ***main*** activities respectively - and the latter MTPDs must, in turn, fall within the respective MTPD for the ***associated*** (parent) ***key product*** / ***service*** / ***operation***

As per the para above - the same applies in principle regarding subordinate ***processes*** and their parent key supporting activities (and likewise [in turn] for subordinate ***procedures*** and their parent processes

Note 4 - Assigned RTOs must fall within (be at an earlier time) than the declared, associated MTPDs for the (associated [parent]) activity in question

Note 5 - Re notes 2 to 4 above. It is 'normal' for a degree of 'juggling / re-adjustment' to take place (as MTPDS and RTOs are estimated - which then have a knock-on effect to their equivalents in the next level above and / or below etc.). This continues until a final, acceptable (to the organisation) result is achieved. Furthermore, every time an MTPD and / or RTO is 'adjusted' as described - a check should be made in case any associated ***MBCO***s require re-adjustment in turn

Step 4

Conduct an assessment aimed at identifying & documenting all actual or potential ***Threats*** which might (if they are 'realised' i.e. actually occur) realistically cause disruption (to a greater or lesser degree) to any ***critical*** / ***critically time-sensitive*** activities (listed in step 3 above)

During the above, some form of (necessarily subjective) 'scoring system' is used to ***estimate*** the ***LIKELIHOOD*** (probability / plausibility / chance / estimation etc.) of each considered ***threat actually happening*** / ***occurring*** - with regard to what the organisation 'does' (i.e. what the nature of its business is)

Whilst the above assessment might logically have been given a title such as '*Threat Analysis*' - it is actually known as '**Risk Analysis**' (admittedly confusing - but this is the accepted term in general use today)

Step 5

The * ***level*** / ***severity*** (using a scoring system similar to that already described further above) of ***IMPACT*** of ***each*** considered ***threat*** on ***each*** considered ***activity*** (should the threat be realised) is then 'combined' with the associated ***LIKELIHOOD*** (typically by means of an associated ** ***matrix***)

The resulting 'scores' represent something known generically as **RISK** - being part of the overarching parent process known as Risk **ASSESSMENT** (of the specific activity being 'assessed')

The results are typically recorded in a document known as a *** **Risk Register**

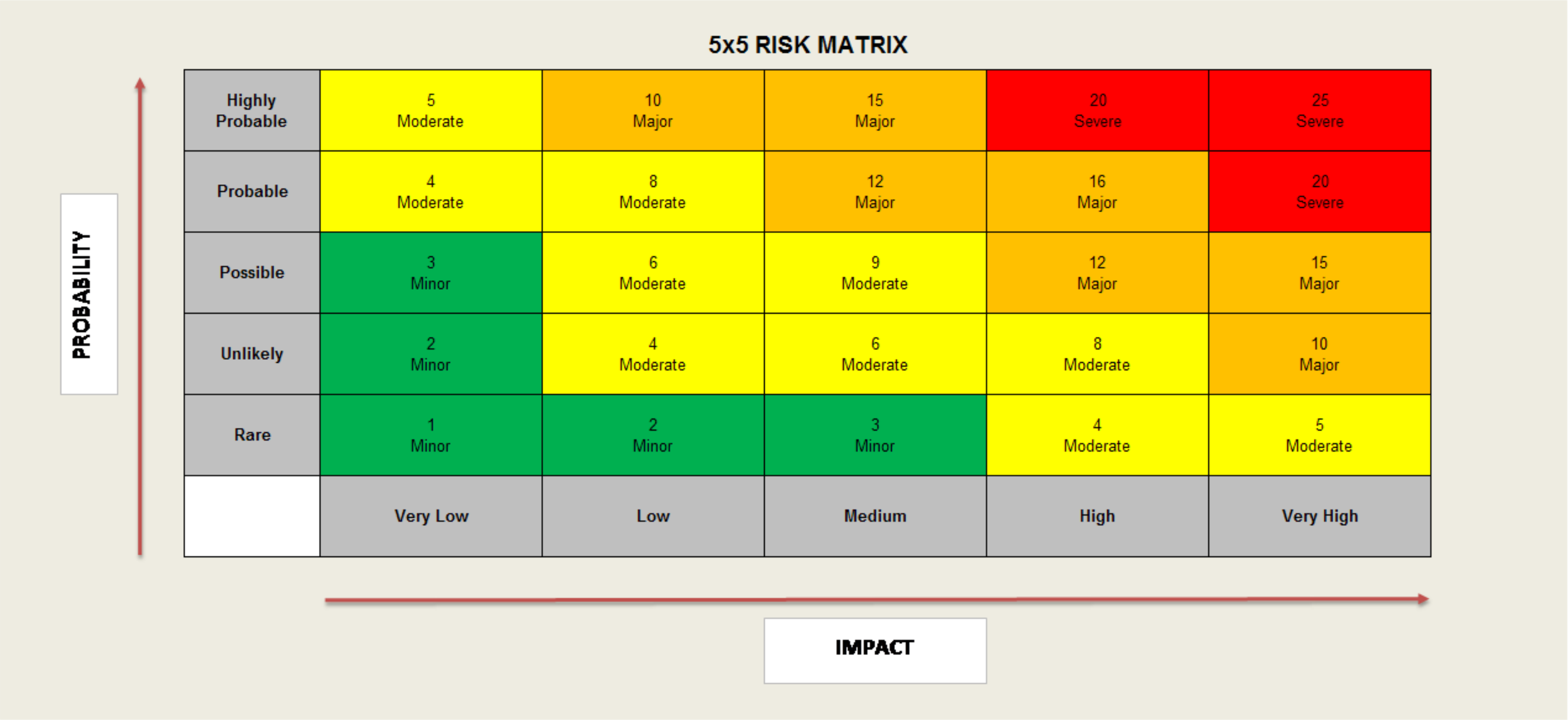
* In a BC context the '***assessment (level) of impact***' is derived from the Step 3 lists (see previous page)

** - For an example of a typical 'risk assessment' matrix - see ***next*** page

*** - For an example of a risk(s) register (this one is for a 'country') - follow the below link:

https://www.gov.uk/government/publications/national-risk-register-of-civil-emergencies-2017-edition

'Risk registers' typically include ***additional*** information describing how individual risks [documented in the register] may be 'mitigated / reduced / avoided' etc.



5x5 RISK MATRIX

PROBABILITY

Highly Probable	5 Moderate	10 Major	15 Major	20 Severe	25 Severe
Probable	4 Moderate	8 Moderate	12 Major	16 Major	20 Severe
Possible	3 Minor	6 Moderate	9 Moderate	12 Major	15 Major
Unlikely	2 Minor	4 Moderate	6 Moderate	8 Moderate	10 Major
Rare	1 Minor	2 Minor	3 Minor	4 Moderate	5 Moderate
	Very Low	Low	Medium	High	Very High

IMPACT

Figure **1a** - '***PROBABILITY***………… versus ***IMPACT***' **Risk Matrix** (coloured (boxed] numeric results indicate the associated levels of resulting risk)

Note 1: Such a matrix would be created (and labelled accordingly) for each and every critical / critically time sensitive activity derived from the Step 3 list - see page 30

Note 2: ***Impact levels*** (V. Low = 1 to V. High = 5 etc.) are shown on the bottom of the matrix running horizontally (and increasing) from left to right. A similar numerical system for ***probability level*** is shown on the left of the matrix running vertically (and increasing) from bottom to top. (Rare = 1 to Highly Probable = 5)

Note 3: The resulting 'risk' scores are obtained by virtually 'drawing' a vertical line upwards from the estimated ***impact*** description (for the particular activity concerned) and a similar (horizontal) ***probability*** line. The coloured box where the two lines meet = the associated level of risk (by number and by name e.g. ***25*** / ***severe***; ***1*** / ***minor*** etc.)

The corners of the above risk matrix chart have the following risk characteristics relating to any selected critical activity etc of concern (e.g. such as those obtained from step 3 on page 30):

- **Bottom Left** - ***Low*** *impact* / ***Low*** *probability* - Can typically (almost always) be ignored

- **Top Left** - ***Low*** *impact* / ***High*** *probability* - The potential risk is going to materialise fairly frequently but will typically be able to ‘managed’ - probably (on most [but not all]) occasions by use of ‘normal business’ type techniques / resources. Nevertheless, reasonably simple and inexpensive measures should ***still*** be implemented to reduce (mitigate) the high ***probability*** factor

- **Bottom Right** - ***High*** *impact* / ***Low*** *probability* - These are high adverse impact risks, but are ***very*** unlikely to happen. Nevertheless, appropriate measures must be taken to reduce (mitigate) the high ***impact*** level (if possible / feasible)

  Additionally, a viable ***business continuity*** solution (plus other appropriate measures if deemed necessary e.g. an emergency [crisis] response plan + associated resources + associated training and exercising etc.) should be put in place - just in case such risks ***do*** materialise

  (A ***catastrophic*** *[mass fatality]* ***aircraft accident*** is a typical example scenario for ***this*** category of risk)

- **Top Right** - ***High*** *impact* / ***High*** *probability* - These are risks are typically classed as ***critical*** (or equivalent description) and must be dealt with as a top priority e.g. the simplest and quickest (but not necessarily acceptable [to the organisation]) solution would be to cease (or possibly not even commence - circumstances permitting) the associated activity altogether

  Otherwise, the organisation must rapidly reduce the predicted levels of ***impact*** and / or ***probability*** to bring the resultant ***risk*** into an ‘acceptable’ range - whatever that might be defined as (by the organisation) - and however it might be achieved. Furthermore, ***business continuity*** measures will also need to be ‘planned for’ - so as to mitigate the resultant risk even further, should it ever be realised

Any other position on the matrix will have impacts / probabilities somewhere within the descriptions covered by the four extremities referred to just above - and should be ‘handled / managed’ as such accordingly - using an appropriate mix of the ‘techniques’ also described

N.B. - in some organisations ***extra attention*** must be given to **very low** ***probability*** risks, where such risks involve ***e.g. potential injury or loss of human life*** type impacts

Furthermore, if such risk ***is*** realised in current media focused times, **immediate and effective *crisis communications*** management by the organisation will be a major consideration - in addition to any other response measures taken. Again, a major airline accident is a good example to refer to here

Step 6

By analysis of data from step 5, decide how to best protect the organisation (by use of various '***Risk*** Treatments ['Controls']) against the various identified risks / threats - after accounting for 'relative impact and likelihood of occurrence' - and also after conducting a 'costs / benefits analysis' as to whether or not it is 'worth' implementing any particular risk treatment

One (**BUT *ONLY*** one) of * several risk treatment / control choices available (particularly for low probability / high impact assessments) is to plan to further ***manage*** the particular risk **AFTER** it has occurred

* Note - see definition of 'Risk Treatments' in (separate document) CRPM Part 3 / Vol 1 Glossary - for a full list of choices

The latter is accomplished (simplistically for now) by use of something known as 'appropriate' ***Business Continuity Strategies*** + their 'associated' ***BC Tactical Solutions / Treatments / Controls*** + associated ***BC Plans** & **Procedures; acquisition of the associated resources required; training and exercising; maintaining; reviewing; continual improvement*** etc.

See below for two examples of what the 6 steps above are typically meant to achieve:

Example 1:

A small organisation's key operational team jointly wins the national lottery and immediately quit their jobs

To account for such a ***risk*** (i.e. unexpected loss of critical manpower) a possible (tactical) *BC treatment / control / solution* might have been to have had other staff (e.g. the boss / line manager etc. of the key staff + admin & support staff etc.) 'cross-trained' to a level where they might have been able to quickly assume some of the more critical responsibilities of the 'quitting' key staff (i.e. *establish a pre-defined level of continuity* [i.e. MBCO - see Glossary] *within pre-defined* [target] *timescales* [i.e. MTPD / RTO - see Glossary] *- until a more appropriate solution could be found*)

More realistically, (and bearing in mind that a small organisation will have few if any 'extra' staff) a better reading of an effectively conducted risk assessment (on the matter concerned) would typically indicate that the chances of winning most national lotteries are extremely low - to such an extent that they can be safely ignored in the situation given above i.e. it will statistically (almost!) never happen

So, the logical / statistical ***Risk Management*** (and thus *BC* solution also) is '***do nothing***' (i.e. ignore the risk)

Example 2:

Following an aircraft accident with mass casualties (i.e. an aviation disaster) to a major, passenger airline - there is a very real (high probability) ***risk*** of associated ICT related 'server meltdown' (associated with the airline's main customer interfacing website[s]) - resulting in extremely slow webpage loading (or even no access at all) - due to the inevitable massive increase in website 'hits' (typically much larger than most airlines could ever imagine!)

Typical (tactical) *business continuity solutions / treatments / controls* for such a situation (risk) might include having (***pre-***established, resourced and implemented) additional server capacity which can be activated at extremely short notice................. and / or employing load shedding (of pre-selected normal business applications) techniques on the website's normal business server(s) - in order to 'make space' for the extra capacity needed for the crisis response etc.

The additional server capacity required should not be underestimated (which ***is*** typically what ***does*** happen when this *BC measure* is planned for and implemented by many airlines)

Furthermore, independent (from the airline's own 'system'), additional / back-up servers should also be utilised - ideally located in a geographical location adequately 'distanced' from where the airline's main server(s) is located e.g. a different country would be good (subject to appropriate checks and 'due diligence' [re this] being accomplished)

Step 7

Implement the decisions (make it happen) made in Step 6 - including provision of a supporting and appropriate response infrastructure, budget, plans, manpower, other resources, information, training, exercising, maintenance, review, audit / compliance, continual improvement etc.

Step 8

Find appropriate methods for dealing with the ***non-critical*** activities as identified in step 2b on page 30. Whilst the latter may not be considered 'critical' (urgent / high importance) - they must nonetheless be accounted for to the extent deemed necessary by top management

An example of a non-critical activity might be an organisation's 'staff restaurant'. Pedantically speaking, ***formal*** BC measures would not be applied to such activity should significant disruption of same arise

However, some form of 'BC' response ***should*** still be pre-considered e.g. this might be as simple as maintaining a contact list of nearby fast food outlets which deliver; having a pre-agreed arrangement for staff to bring their own food / refreshments to work etc.

Steps 1 to 8 (above) are shown in simple flow diagram format on the ***next*** page

Reminder - the above (pages 28 - 35) is merely a ***very simplistic*** overview

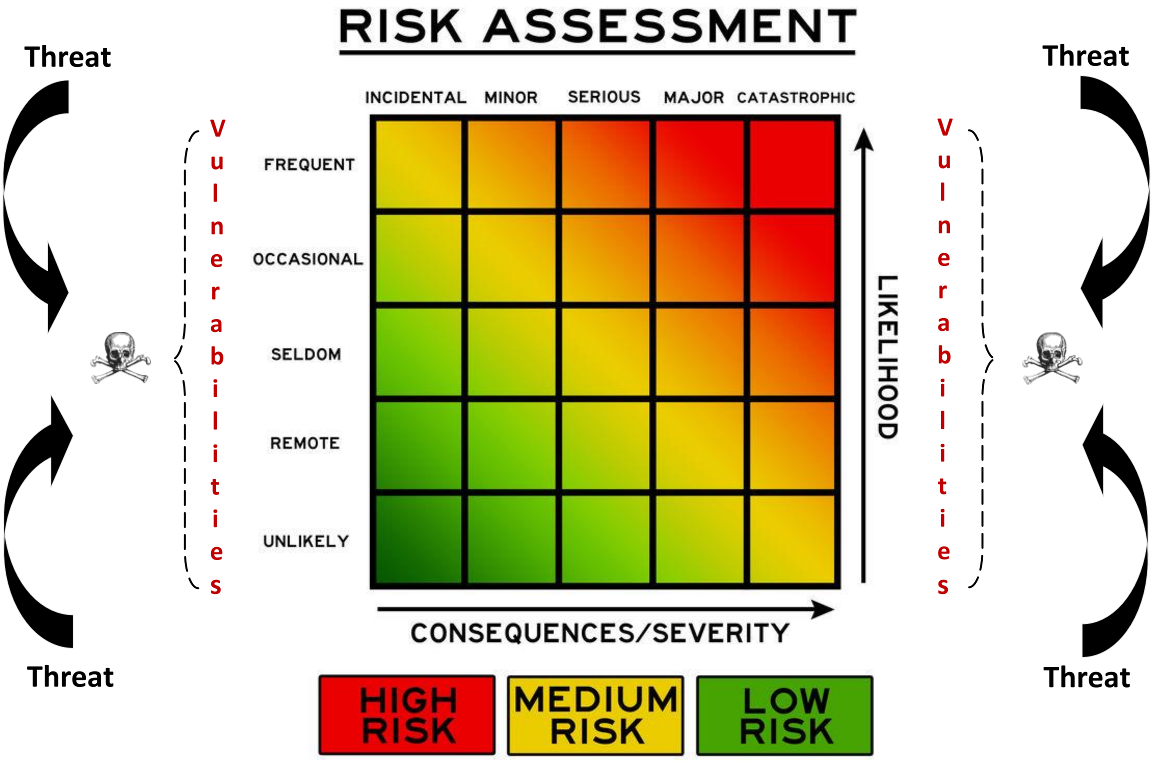
That said, the above ***could*** work (with a little expansion, time, effort and some [not too much] expenditure) ***e.g. for a small, regional passenger airline flying several aircraft*** (e.g. 20-30 seaters) ***on short-haul routes - between non-complex airports - and in a part of the world where potential threats / hazards / vulnerabilities to such operation are relatively rare***

Remember:

Threat **is the potential harm which *might* impact on an asset** (what you're trying to protect)

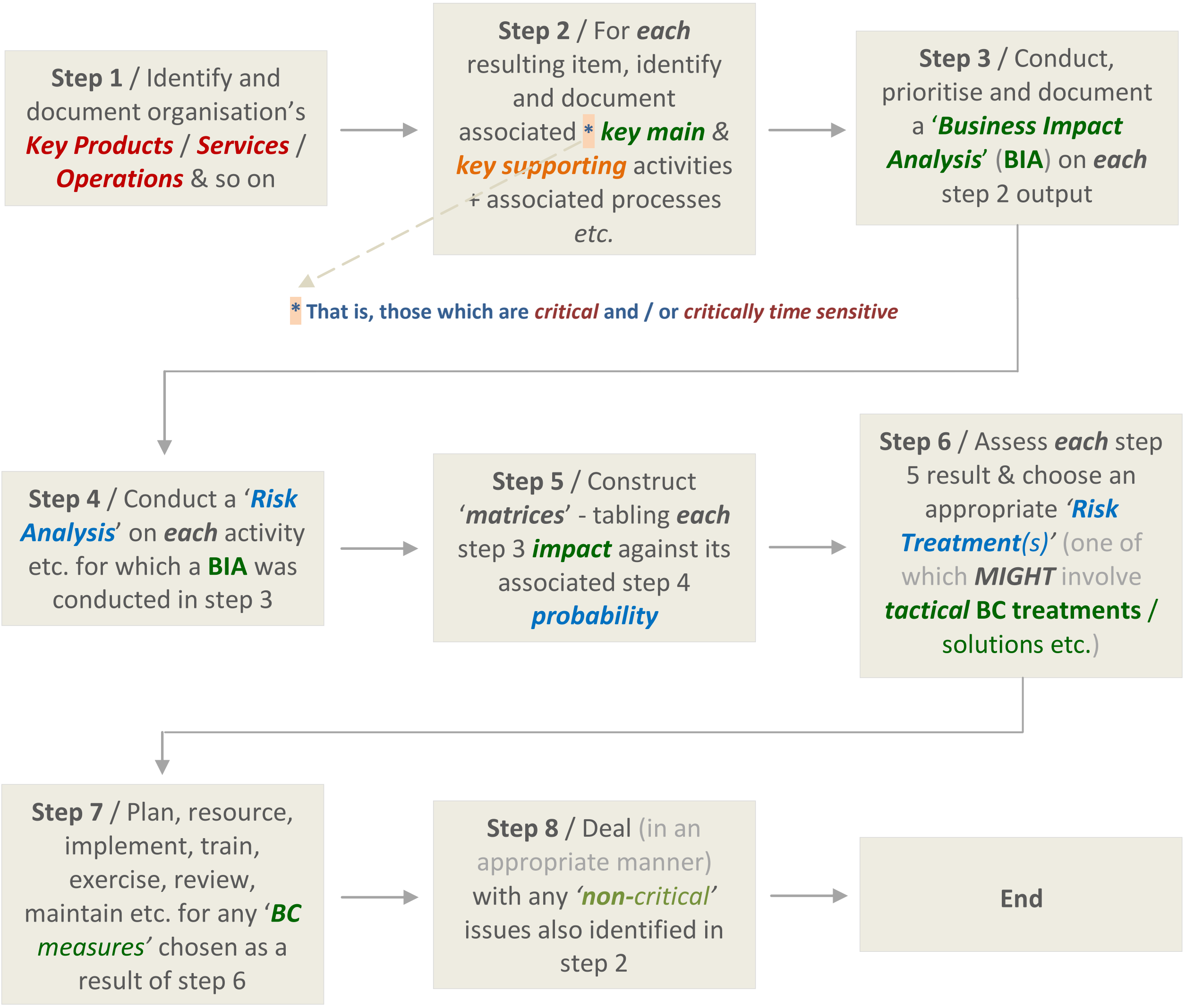
Risk **is the probability** (likelihood etc.) **that the harm will be realised** (will actually occur) **- and**

Vulnerability **is a weakness by which an associated threat might be realised and thus** (then) **be able to potentially impact upon the asset - typically causing it harm**



Simplified Flow-Chart

Introducing a BCMS into a Small to Medium sized (non-complex) Organisation



Step 1 / Identify and document organisation's ***Key Products*** / ***Services*** / ***Operations*** & so on

Step 2 / For *each* resulting item, identify and document associated * ***key main*** & ***key supporting*** activities + associated processes *etc.*

Step 3 / Conduct, prioritise and document a '***Business Impact Analysis***' (**BIA**) on *each* step 2 output

* That is, those which are *critical* and / or *critically time sensitive*

Step 4 / Conduct a '***Risk Analysis***' on *each* activity etc. for which a **BIA** was conducted in step 3

Step 5 / Construct '***matrices***' - tabling *each* step 3 ***impact*** against its associated step 4 ***probability***

Step 6 / Assess *each* step 5 result & choose an appropriate '***Risk Treatment(s)***' (one of which ***MIGHT*** involve ***tactical* BC treatments** / solutions etc.)

Step 7 / Plan, resource, implement, train, exercise, review, maintain etc. for any '***BC measures***' chosen as a result of step 6

Step 8 / Deal (in an appropriate manner) with any '***non-critical***' issues also identified in step 2

End

Figure **1b**

- 'Notes 1 to 5' on page 30 likewise apply to 'Steps' 1, 2 and 3 above

- The initial steps re any BC related output(s) from step 6 are otherwise known *(perhaps confusingly)* as '………*setting business continuity* **strategy** & **solutions**………'

- Reminder - business continuity planning matters concerning ***data*** loss / recovery (both soft and hard copy) are outside the scope of this guideline document - *but* **MUST** *obviously be accounted for in reality*

Before we leave this **Evolution of BC** sub-section it is worth reinforcing (again) where 'Business Continuity' most definitely 'sits' with regards to 'Risk Management'. You can do this by having a 'good read' of the article found at the end of the following link:

https://www.bcpbuilder.com/2018/11/21/business-continuity-risk-management/

……………………………..and a study of the diagram shown just below:

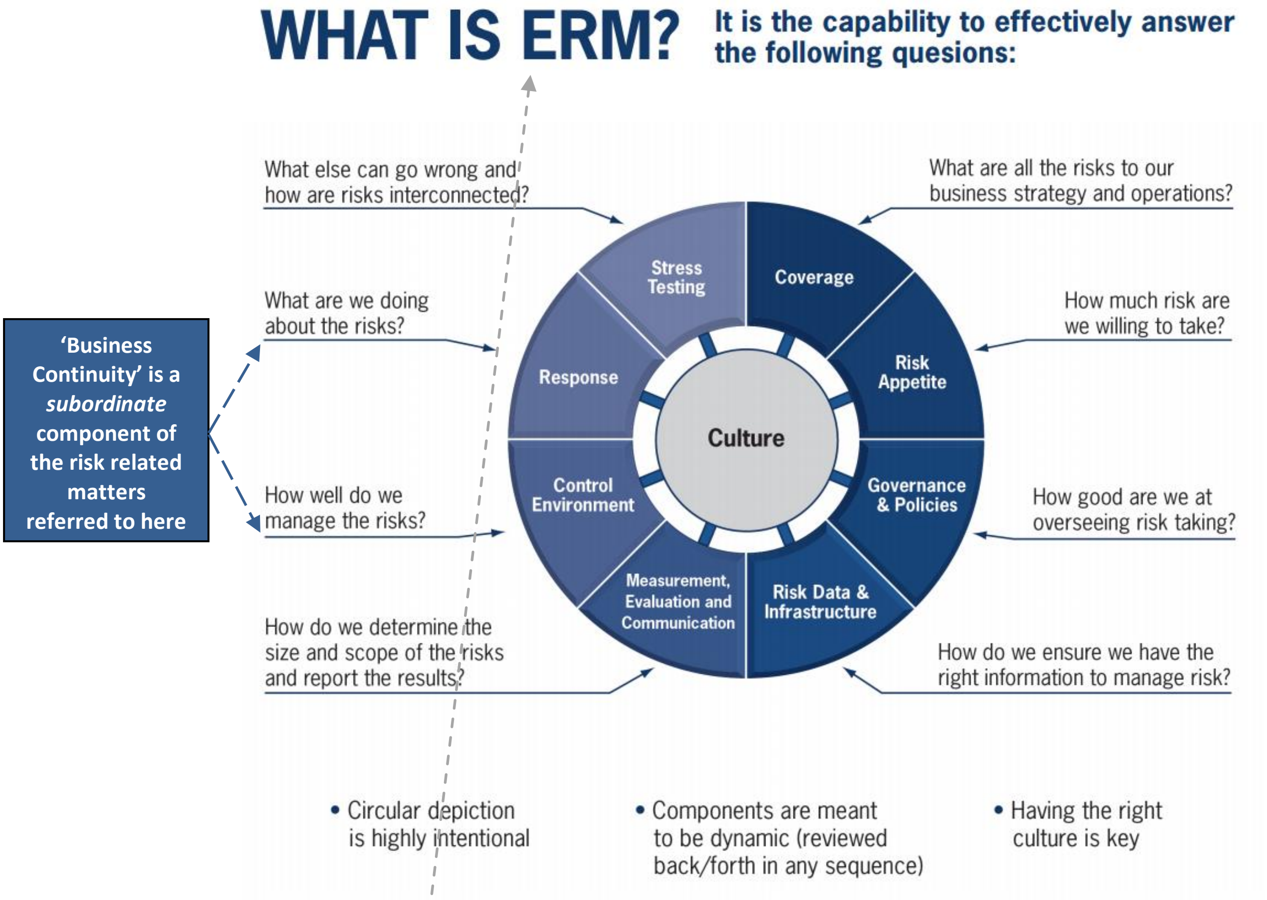

WHAT IS ERM?
It is the capability to effectively answer the following quesions:
What else can go wrong and how are risks interconnected?
What are all the risks to our business strategy and operations?
What are we doing about the risks?
How much risk are we willing to take?
How well do we manage the risks?
How good are we at overseeing risk taking?
How do we determine the size and scope of the risks and report the results?
How do we ensure we have the right information to manage risk?
Stress Testing
Coverage
Risk Appetite
Governance & Policies
Risk Data & Infrastructure
Measurement, Evaluation and Communication
Control Environment
Response
Culture
• Circular depiction is highly intentional
• Components are meant to be dynamic (reviewed back/forth in any sequence)
• Having the right culture is key
'Business Continuity' is a *subordinate* component of the risk related matters referred to here

Image above via 'apollohr.com'

Figure **1c**

For a definition of **E**nterprise **R**isk **M**anagement - see (***separate*** doc) CRPM Part 3 / ***Vol 1*** - Appendix A2

When ***this*** document (the one you are reading right now i.e. CRPM Part 3 / ***Vol 2***) refers to 'risk management' - it ***is*** typically referring to 'ERM' - unless stated otherwise

Has BC Become Unnecessarily Complex?

Having just seen (hopefully!) how ***relatively*** simple BC might be - it is worth contrasting here for a moment the 'unnecessary complexities' associated with most of the current (ISO) BC related standards, related 'commercial' guidance material and similar - intended to guide the process of introducing BC (a BCMS) into an organisation. As an example, take ISO 22313 (***Guidance*** to achieving associated ISO 22301 ***Requirements***)

When ISO 22313 was (first) issued as a 'brand new' BC standard in late 2012 - the intent was to take the best of its 'predecessor' standards, in order to come up with a new, universal BC standard which was 'fit for purpose'

The author / owner (of this guideline document) is of the opinion that ISO 22313 (then [2012 version] and ***also*** now in its February 2020 evolution) was / is still unnecessarily difficult for the layperson to understand (both in its written word and also its 'meaning')

It might also present similar 'understanding difficulties' to some who are more 'professionally' involved with the subject - the author / owner (of this guideline document) being an example!

> Accordingly, ***this*** guideline document (the one you are reading now) has tried its best to use wording etc. consistent with the average layperson user / reader being able to at least have a better chance of grasping the meaning of same at first or second reading
>
> The latter would be significantly facilitated when combined with an appropriate training course based on ***this*** guideline document (such training etc. is essential for those really serious about aviation related BC)
>
> Nevertheless, it is acknowledged that the wording (and associated meanings) used in ***this*** guideline document itself may still (at least in places) not be as clear and simple as is desired - particularly for the non-native English speaker
>
> Accordingly, feedback on how such wording, meanings etc. may be further clarified / simplified will be gratefully received at: '*info@aviation-erp.com*'

Reminder - the above comments are based on the author / owner's personal thoughts. Many readers (especially 'BC professionals') will no doubt disagree with him on this matter. For more details - see (separate) document CRPM Part 3 / ***Volume 1*** / ***Note 4*** *(starts page 33)*

Importance of BC (a BCMS)

Business Continuity (or more relevantly - the concept of a 'Business Continuity Management System' [BCMS]) emphasises the importance (to the organisation concerned etc.) of:

- Top management assuming the associated BCMS leadership accountabilities etc.
- Other involved persons attaining and retaining the required knowledge, skills, experience etc. (competence; exercising; real occurrences etc.)

- Identifying and understanding the organisation's business objectives
- Establishing business continuity scope (including exclusions), policy etc. - in accordance with the above business objectives
- Operating, maintaining and improving processes, capabilities and response structures so that the organisation might better survive disruptions e.g. via analysis, strategy setting, providing associated resources (incl. budget and an appropriate response structure[s]), establishing appropriate plans and procedures, establishing competence and experience, creating and maintaining associated documentation etc.
- Monitoring, reviewing etc. the performance and effectiveness of the BCMS
- Continual improvement based on associated qualitative & quantitative measurement

Potential Benefits of BC (a BCMS)

To ***recap what has already been covered so far***, some organisations typically use 'business continuity' measures to better identify and 'understand' their key products / services / operations etc. + the latters' associated (subordinate) component activities / processes / procedures / resources etc.

From this it is possible to make an 'informed / educated guess' of the (typically negative / adverse) ***IMPACT****(s)* (on the organisation) should such products / services etc. be ***disrupted*** (for whatever reason) for a '***significant***' period of time

Similarly, ***THREATS*** to an organisation's key products etc. (together with the associated ***vulnerabilities***) are identified and a further 'informed / educated guess' made as to the ***PROBABILITY*** of such threats being realised (i.e. actually occurring)

The results are recorded in a document known as a 'risk register (updated as required)

Concerning any particular product / service / operation etc. - the ***impact*** & ***probability*** 'scores' from above are '***merged*** / ***combined***' in such a way (typically by plotting on something known as a 'risk' matrix) that the organisation can use the results to better manage risk, by use of various 'treatments / solutions / controls'

One (but ***ONLY*** one of several) of such risk treatments / solutions / controls etc. is based on use of appropriate and associated ***Business Continuity*** measures

How the risk is planned to be 'managed / mitigated' is also typically documented in the appropriate part of the associated risk register

All of the above enables the organisation ***to be better prepared for*** *'****the worst****' by* ***taking associated countermeasures*** *(if it wants to) in order to improve its* ***RESILIENCE***

Additional benefits of introducing a BCMS into an organisation potentially include:

- ***Enhanced protection*** of e.g. life, assets, the environment etc.
- Compliance and assurance with the expectations of ***legislators, regulators, insurers, business partners, shareholders*** and other ***key stakeholders*** / ***interested parties***
- ***Essential services maintained during actual disruption*** - ***hence customer service*** (meeting customer requirements) ***and*** (probably) ***customer loyalty is maintained / retained***. (This is 'marketable' of course and can be used to retain current customers & attract new ones [see Case Study 5 {page 279} for a real-life example of this])
- ***Adverse financial impacts minimised*** - when disruptions ***do*** occur
- (As applicable) - Better ***management of the 'supply chain'*** and ***identification of any associated weaknesses*** (+ also maintaining the confidence of suppliers)
- Improving understanding, monitoring & management of '***risk***' in general (including the possibly beneficial applications of 'risk appetite')
- ***Competitive advantage*** opportunities (compared to competitors ***not*** embracing BC)
- ***Financial benefits*** due identification and rectification of organisational weaknesses e.g. single point(s) of failure, duplications etc.
- ***Information*** / ***data assets secured***
- ***Reduced insurance premiums*** / ***wider insurance cover*** / ***less onerous excesses***
- Organisational objectives continuing to be met ***via the ability to manage disruption***
- Identifying the most effective & efficient ways of working = ***a 'leaner' organisation***
- ***The embedding of BC 'awareness and competence' throughout an organisation***. This is particularly useful in eliminating any residual weaknesses and 'single points of failure' missed during the BIA - and can also contribute to improved processes, resilience and job satisfaction / morale
- ***Reputation*** / ***brand*** / ***image*** / ***credibility*** type matters (maintained or even improved) by demonstrating a professional approach to effectively & efficiently managing adverse situations - possibly (based on limited empirical evidence) accompanied by a post-disruption rise in the value of the organisation's stocks & shares (the opposite might also apply of course!)
- ***Job security improved*** via the creation / continuance of a sustainable organisation

Note 1 - above list is ***not*** exhaustive. ***Note 2*** - Above list is slanted more towards the ***private*** sector than the ***public*** sector. The latter should be accounted for this accordingly - when studying / using ***this*** guideline document. ***Note 3*** - The interested reader might also wish to take a look at ISO 22313:2020 itself, para 0.2, starts page vii

Wish-list of BC (BCMS) **Outcomes** - Cross Reference - ISO **22313** / 9.1.4

Now might be a good time for the user / reader to become aware (in general terms at least) of what (according to ISO 22313:2020) successful introduction of a BCMS into a typical medium to large sized organisation should / might have accomplished when such project is 100% complete (i.e. what it should be producing in the way of what might be termed '***BC Outcomes***')

Doing this will hopefully provide some valuable context (up to this point) in the study of this guideline document. ***The list is not exhaustive*** and in no particular order. Refer to the glossary in our (***separate*** document) 'CRPM Part 3 / Volume 1' - where necessary:

- ✓ ***Top-management fully 'on-board'*** - insofar as BC matters are concerned

- ✓ ***An adequate number of staff*** / ***people*** (e.g. consultants) ***with suitable*** / ***appropriate knowledge, skills, experience etc. are*** / ***remain available*** to adequately plan for, document, resource, implement, train, manage, operate, exercise, maintain, evaluate and continually improve the organisation's BCMS

- ✓ From a BC viewpoint / context, the organisation's requirements ***to fully understand 'itself' internally*** - together with a similar understanding of the context & other details of ***how it will need to interact*** / ***inter-relate with all appropriate external 'interested' parties*** (including 'stakeholders') - has been adequately researched, developed, documented, understood, accounted for, trained for, exercised for etc. (Also see definition 'Understanding the Organisation' [CRPM Part 3 / ***Volume 1*** glossary refers] + the info provided on page 53 of ***this*** document [i.e. the one you are reading now])

- ✓ ***Supply chain*** (if appropriate) adequately ***secured***

- ✓ A fully functional / effective (fit for purpose) '***incident response structure***' is in place - ready to deal with the ***immediate*** consequences of whatever was the ***initial*** cause of a disruption - as / if appropriate (i.e. direct ***emergency*** / ***crisis*** response [if so required] must **ALWAYS** come first - * and ***only*** then followed by any associated (but separate) ***business continuity*** / ***business recovery*** and similar issues - as required)

  * Unless (***exceptionally***) circumstances 'on the day' are such that the organisation can ***adequately*** manage / respond etc. to all such requirements concurrently

IMPORTANT NOTE

Re '***incident response structure***' - it is ***strongly*** suggested that the 'interested' reader refreshes his / her memory (as required) of the associated meaning of this term as used herein (see glossary of [***separate*** document] CRPM Part 3 / ***Volume 1***)

Whilst so doing, he / she might also wish to review the info entitled '***Concurrent BCP Ops + ERP Ops + Normal Business Ops***' referred to on page 43 of said Volume **1**

- ✓ Fully functional ***business continuity*** and ***business recovery*** plans and procedures are in place - which have identified the organisation's key products / services / ops, have been designed and prepared to protect the latter (from disruptive risk) insofar as is desired / possible / practicable - and, ***post-disruption*** will assist in ***returning*** (recovering) ***the organisation to normal operations*** without unacceptable delay

- ✓ ***BC is adequately resourced*** - including adequate and appropriate finance / budget, manpower, facilities, equipment, ICT, supporting services etc.

- ✓ ***BC awareness, competency and exercise programmes fully established and maintained*** - including a documented training (initial & recurrent) and exercise (recurrent) operation

- ✓ Organisation ***compliant*** with all appropriate legal, regulatory, best / good practice and similar requirements (as required for latter two)

- ✓ A robust, documented ***BC communications plan*** (internal & external) is in place

- ✓ The preservation of the organisation's '***brand, image, reputation and credibility***' has been adequately considered and provided for

- ✓ ***Financial controls are maintained*** throughout a BC related occurrence

- ✓ ***BC performance consistently maintained and evaluated***

- ✓ ***Continual improvement*** (on-going) of the BCMS (and thus ***Resilience***) is evidenced and documented

- ✓ All of the above is adequately and securely ***documented***

Review of BCMS outcomes by top management should be regularly scheduled and evaluated

For a 'dose of reality' related to users / readers with an **airport** background (might be of interest to aircraft operators [airlines etc.] and GHAs too) - see the info found at the end of the below link. The article was written in 2011 (but the situation described had not changed significantly as at 2020!)

http://www.continuityforum.org/content/news/147709/5-steps-avoid-airport-misery

Deliberately Blank

Section 3 / (* Modern) **MANAGEMENT SYSTEMS**

PDCA CYCLE

In common with other types of 'modern' management systems (MMS) - this guideline refers to and uses the '***PLAN → DO → CHECK → ACT*** (PDCA)' cycle (see ISO 22313:2020, paras 0.3 & 0.4 [pages 'viii' and 'ix' respectively])

The latter is a high level 'road map' type concept for standardising the planning, documenting, resourcing, establishing / implementing, training, managing / operating, exercising, maintaining and evaluating of (in this case i.e. as used herein) ………………… an organisation's BCMS. As a concept, it has the ultimate aim of achieving continual improvement leading, in turn, to continually increasing 'customer' satisfaction

Whilst we use the PDCA herein specifically for BCMS related purposes, the concept is today similarly (typically) applied to all other 'types' of ***modern*** management system (e.g. Quality Management System; Environmental Management System etc.) in use around the world

* For a reminder of what the term 'modern management system' means - see [***separate***] document CRPM Part 3 / ***Volume 1*** - page 79

Note 1: See 'important note' - page 18 of the document you are reading now. **Note 2**: Numerous cross-references (predominately for the purposes of context) are made herein to ISO 22313:2020. ***The 'serious' reader / user would benefit significantly from having ready access to the latter***

Whilst ISO 22313:2020 can be purchased, a thorough internet search (using appropriate keywords) **might come up with what is required, at no cost** (such search is likely to become more successful commensurate with the time period passed since the document was first published in February 2020). **However, do keep in mind that all ISO documents and equivalents are copyright protected so caution in such matter is advised**

The *PDCA* Cycle

Plan (PRE-plan / Plan for etc. Ref ISO 22313 clauses 4 to 7) = ***research/identify/document*** etc. BC requirements and all associated matters - as outlined in the '**PLAN**' Box - figure 4, page 51

Do = ***Implement / action & operate*** all of the above (Make it happen etc. Ref ISO 22313 clause 8) - as outlined in the '**DO**' Boxes - figure 4, pages 51 & 52

Check = ***Monitor & review*** (Evaluate. Ref ISO 22313 clause 9) BC performance against BC policy, objectives etc. + practical (real life) experience (feedback) etc. of BC 'in action'

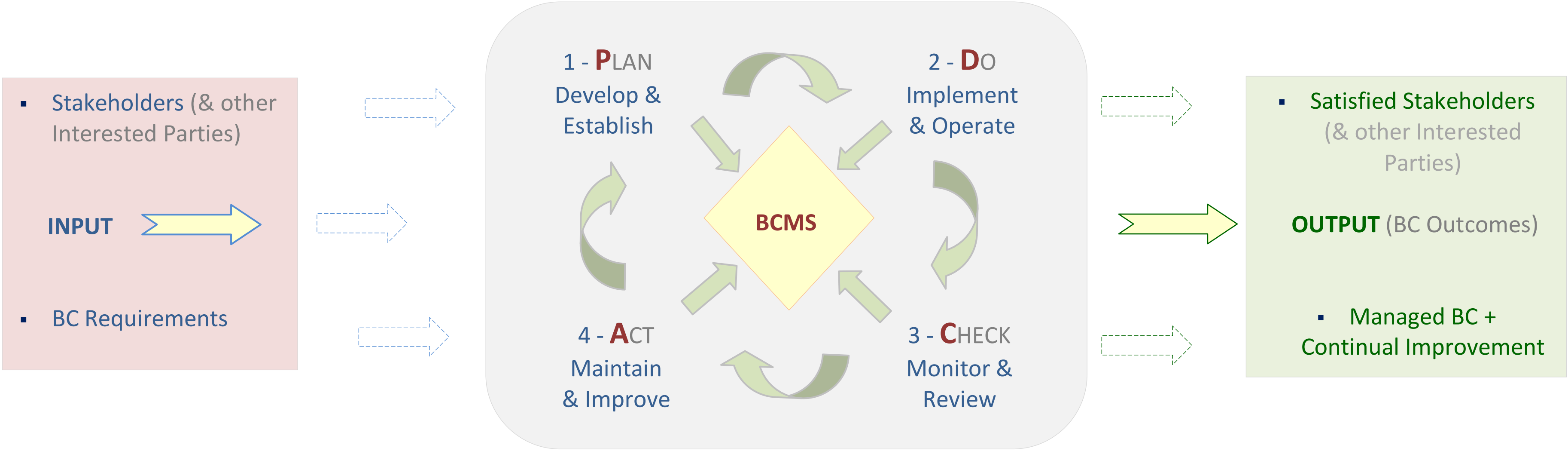
Present results for review by top management and determine, authorise, resource and enact all remedial measures required to achieve continual improvement, thus continually improving customer satisfaction - as outlined in the '**CHECK** & **ACT**' Box - figure 4, page 52

Act = ***Maintain & improve*** the BCMS (Ref ISO 22313 clause 10) by use of:

- The 'corrective / * preventive action' system common to all modern management systems
- By implementing the recommendations from reviews by top management and others……………….and
- By periodically (and / or as required) re-appraising the scope of the BCMS, together with BC policy and objectives - also as outlined in the '**CHECK** & **ACT**' Box - figure 4, page 52

* Note - '***Preventive action***' is actually an integral part of the (***non-BC related element***) of '***risk management***' and is thus ***not*** pedantically a component of business continuity. However, it is obviously a significant consideration to account for and is thus expanded upon later herein (see related info starting pages 77 and 256)

The PDCA cycle should operate ***indefinitely*** via its on-going BCMS ***programme management*** elements (*latter otherwise known as the '**BCMS life-cycle**'*) (see pages 48 and 49). For example, there will always be a need for new or revised policies & objectives; targets & controls will change; maintenance is a constant requirement - as are training, exercising, monitoring & review; threats will come and go - as will their associated vulnerabilities etc.



- Stakeholders (& other Interested Parties)

INPUT

- BC Requirements

1 - PLAN
Develop & Establish

2 - DO
Implement & Operate

BCMS

3 - CHECK
Monitor & Review

4 - ACT
Maintain & Improve

- Satisfied Stakeholders (& other Interested Parties)

OUTPUT (BC Outcomes)

- Managed BC + Continual Improvement

Figure **2** / **PDCA Cycle** as related to a BCMS

Typical ***Core Elements*** of ***BC Programme Management*** (BCMS Life-Cycle)

Cross Ref - ISO 22313 / 8.1 / 'Operational Planning & Control'

The BC ***Programme Management*** (BCMS Life-cycle) diagram (fig. 3 next page) portrays the ***core*** elements of same - as described (in greater detail) later in this guideline

A shorter term objective here (for now) is to try to assist the user / reader in acquiring a relatively basic understanding of the meaning & application(s) of each labelled element (in fig. 3) - both individually and as related to * other (***sub-core***) elements, as appropriate

Not shown in figure 3 (but nevertheless to also be adequately accounted for) are:

- The setting of an appropriate scope and policy for the BCMS + establishment of associated BCMS objectives
- Effective operational planning & control - led by an appropriately competent, knowledgeable, experienced etc. person(s) (might need to be sourced externally?) - typically appointed / engaged by top management

* Note - Each ***core*** element is, in turn, made up of ***sub*-core** elements - a representative list of the latter being shown in the 'figure 4' diagram - pages 51 & 52

Note - from this point on (in this guideline document i.e. the document which you are reading now), the PDCA cycle, as it applies in turn to each labelled element of BC programme management (see definition below & diagram next page) + the two bullet points just above, should be considered to be continually applied - for as long as the BCMS is in use within the organisation

Reminder: (Definition)

- **Business Continuity** (BC) **Programme Management**

  An on-going (***cyclical***) governance & management process (supported by an organisation's top management & appropriately resourced) intended to implement, maintain, review and continually improve an organisation's BCMS i.e. improve '***organisational resilience***'

  For an excellent explanation of what is meant by the term 'organisational resilience' - follow the below link:

  https://www.thebci.org/news/what-is-organisational-resilience.html

PDCA Cycle - **Business Continuity Management System**

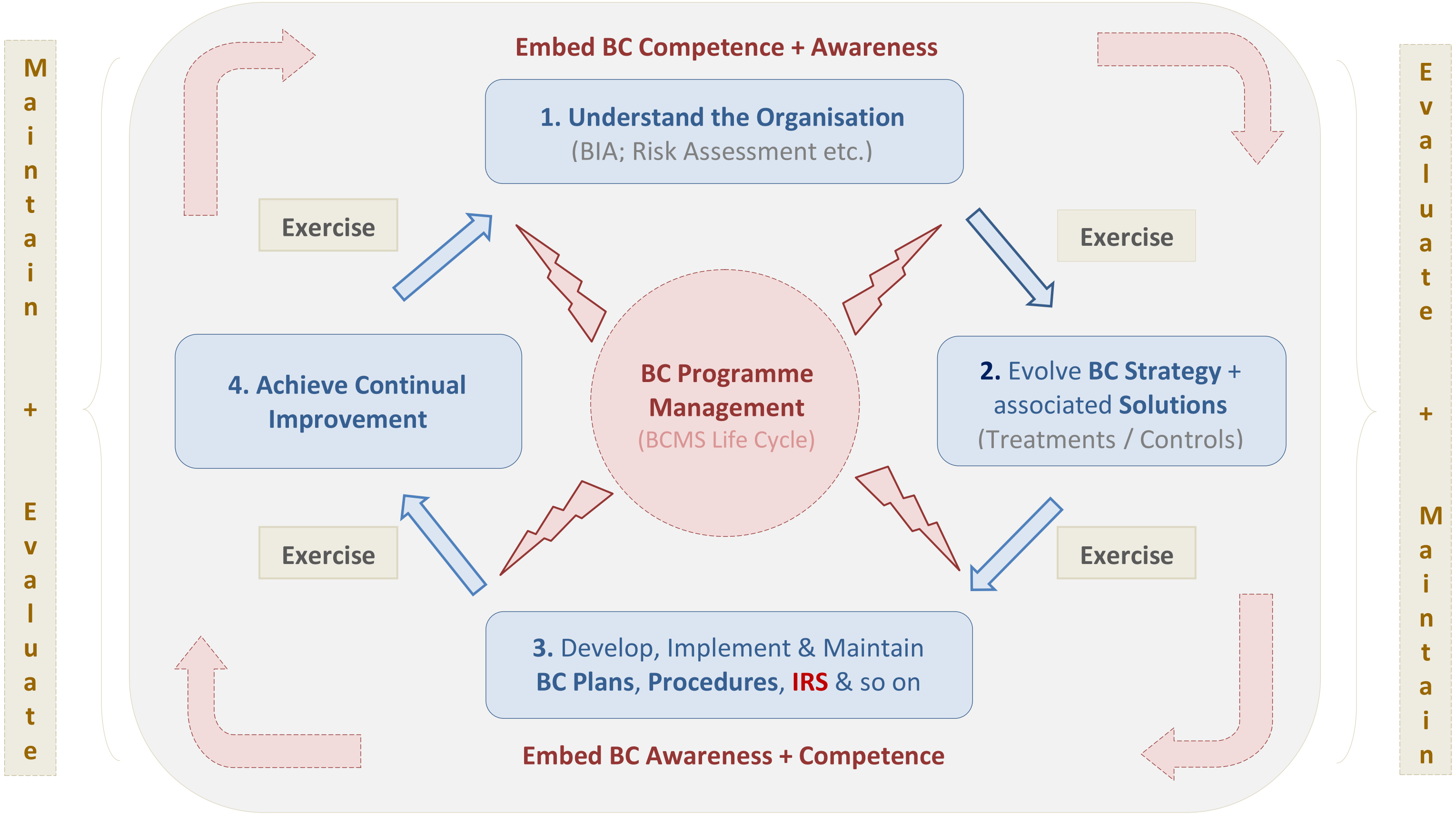

Maintain + Evaluate
Embed BC Competence + Awareness
1. Understand the Organisation
(BIA; Risk Assessment etc.)
Exercise
Exercise
Evaluate + Maintain
4. Achieve Continual Improvement
BC Programme Management
(BCMS Life Cycle)
2. Evolve BC Strategy + associated Solutions
(Treatments / Controls)
Exercise
Exercise
3. Develop, Implement & Maintain
BC Plans, Procedures, IRS & so on
Embed BC Awareness + Competence

Figure **3** - Typical *'**core elements**'* of ***BC Programme Management*** (otherwise known as the *'**BCMS Life Cycle**'*)

The organisation should determine, plan, implement and control those actions (processes) needed to establish and maintain its BCMS (policy, objectives etc.) - in conjunction with the associated '***context of the organisation***' (derived as per ISO 22313:2020 / clause 4) + the chosen level of '***risk appetite***', if any (derived as per ISO 22313:2020 / clause 6.1)

Such actions (processes) are used to create an associated 'programme' (as per definition of 'BC Programme Management' shown on page 48) - which guides their integration into the organisation's 'normal business' processes, in order that they might be 'managed' appropriately, their effectiveness maintained etc.

Notes below refer to figure 3 on the previous page:

Note 1 - '***Embed BC Awareness & Competence***' in an organisation = the on-going tasks of:

- ***Top Management's*** absolute commitment and support to / for the BCMS
- Ensuring ***ALL*** staff gain a reasonable awareness of the BCMS and its objectives
- Ensuring ***nominated*** staff are 100% aware of their BCMS roles & responsibilities
- Ensure ***nominated*** staff acquire and retain appropriate BCMS competencies
- Ensure ***nominated*** staff periodically exercise their BCMS roles & responsibilities

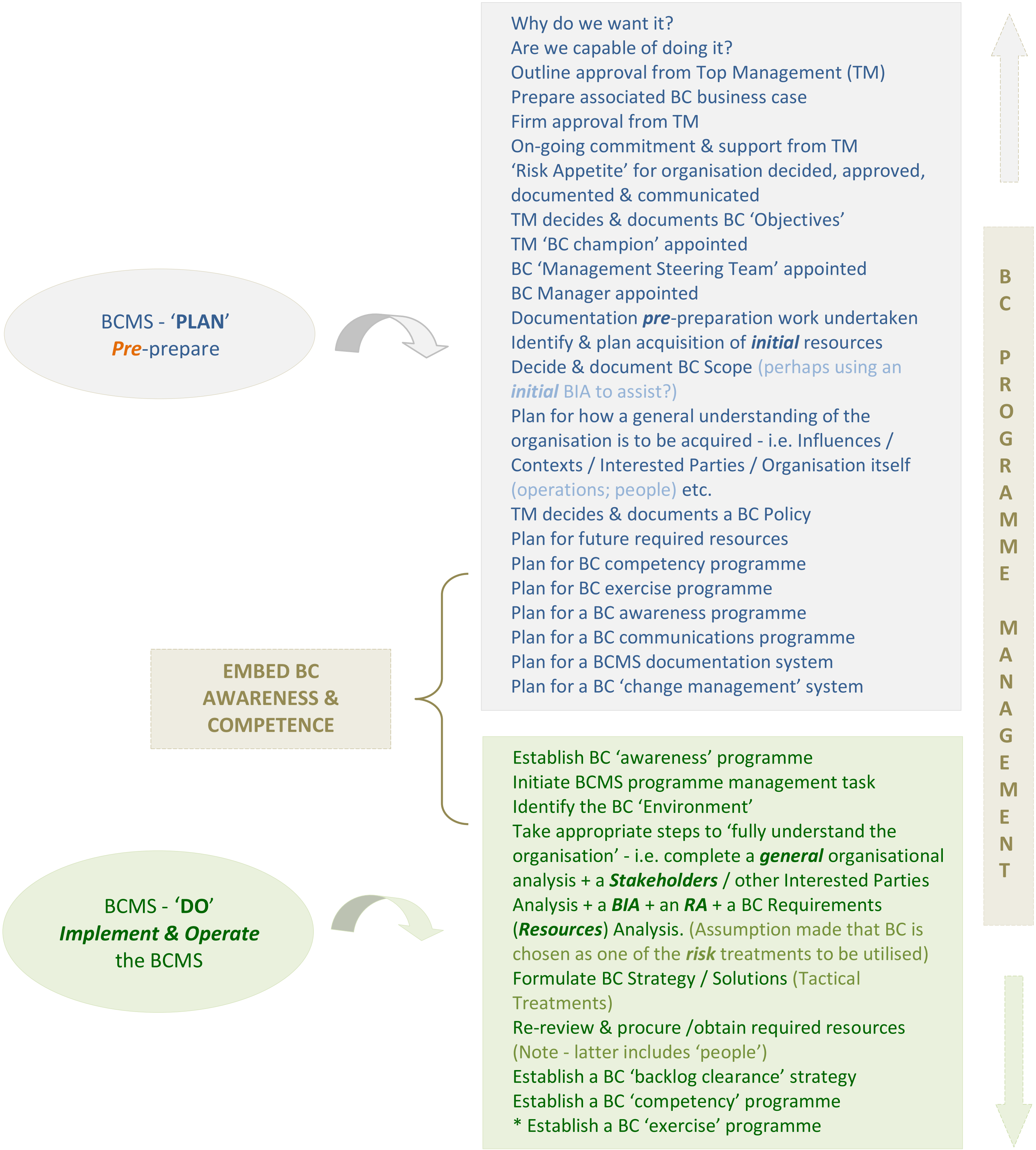
Note 2 - for an explanation of what is interpreted in ***this*** guideline document as '***understand the organisation***' - see the note on page 53

Note 3 - differing terminology for 'BC Programme Management / BCMS lifecycle' (than that shown in the diagram on the previous page) may still be in use in some organisations / documents etc. in different parts of the world e.g. (typically):

- 'BC Programme Management' might be alternatively termed '***BC Policy and Programme Management*** *or* '***Processes Required to Establish and Maintain BC Management***'
- 'Understanding the Organisation' might be alternatively termed '***Analysis***'
- 'Selecting BC Strategy & Solutions / Tactical Treatments' etc. might be alternatively termed '***Design***'
- 'Maintain, evaluate and review' may be alternatively termed '***Validation***'

Typical ***Sub-core*** Elements of BC Programme Management

See figure 4 (next ***two*** pages):



BCMS - ‘**PLAN**’
Pre-prepare

Why do we want it?
Are we capable of doing it?
Outline approval from Top Management (TM)
Prepare associated BC business case
Firm approval from TM
On-going commitment & support from TM
‘Risk Appetite’ for organisation decided, approved, documented & communicated
TM decides & documents BC ‘Objectives’
TM ‘BC champion’ appointed
BC ‘Management Steering Team’ appointed
BC Manager appointed
Documentation ***pre***-preparation work undertaken
Identify & plan acquisition of ***initial*** resources
Decide & document BC Scope (perhaps using an ***initial*** BIA to assist?)
Plan for how a general understanding of the organisation is to be acquired - i.e. Influences / Contexts / Interested Parties / Organisation itself (operations; people) etc.
TM decides & documents a BC Policy
Plan for future required resources
Plan for BC competency programme
Plan for BC exercise programme
Plan for a BC awareness programme
Plan for a BC communications programme
Plan for a BCMS documentation system
Plan for a BC ‘change management’ system

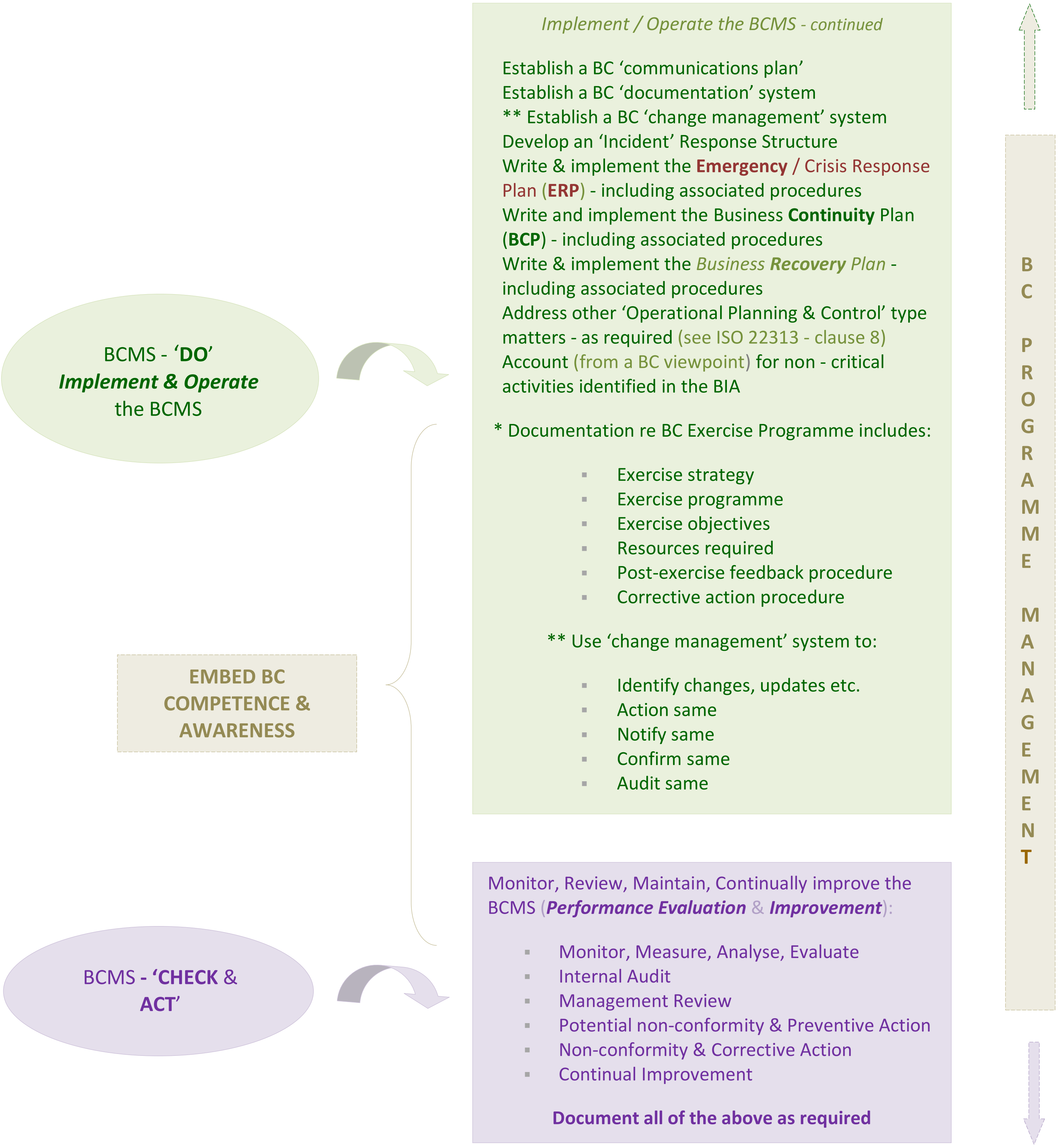
EMBED BC AWARENESS & COMPETENCE

BCMS - ‘**DO**’
Implement & Operate
the BCMS

Establish BC ‘awareness’ programme
Initiate BCMS programme management task
Identify the BC ‘Environment’
Take appropriate steps to ‘fully understand the organisation’ - i.e. complete a ***general*** organisational analysis + a ***Stakeholders*** / other Interested Parties Analysis + a ***BIA*** + an ***RA*** + a BC Requirements (***Resources***) Analysis. (Assumption made that BC is chosen as one of the ***risk*** treatments to be utilised)
Formulate BC Strategy / Solutions (Tactical Treatments)
Re-review & procure /obtain required resources (Note - latter includes ‘people’)
Establish a BC ‘backlog clearance’ strategy
Establish a BC ‘competency’ programme
* Establish a BC ‘exercise’ programme

Figure **4** - PDCA’s cyclical relationship with BCMS ***planning***, ***implementation/operation***, ***monitoring/reviewing*** and ***maintaining/improving***

Figure **4** - continued



Implement / Operate the BCMS - continued

Establish a BC 'communications plan'
Establish a BC 'documentation' system
** Establish a BC 'change management' system
Develop an 'Incident' Response Structure
Write & implement the **Emergency** / Crisis Response Plan (**ERP**) - including associated procedures
Write and implement the Business **Continuity** Plan (**BCP**) - including associated procedures
Write & implement the *Business **Recovery** Plan* - including associated procedures
Address other 'Operational Planning & Control' type matters - as required (see ISO 22313 - clause 8)
Account (from a BC viewpoint) for non - critical activities identified in the BIA

* Documentation re BC Exercise Programme includes:

- Exercise strategy
- Exercise programme
- Exercise objectives
- Resources required
- Post-exercise feedback procedure
- Corrective action procedure

** Use 'change management' system to:

- Identify changes, updates etc.
- Action same
- Notify same
- Confirm same
- Audit same

BCMS - '**DO**'
Implement & Operate
the BCMS

EMBED BC COMPETENCE & AWARENESS

Monitor, Review, Maintain, Continually improve the BCMS (***Performance Evaluation*** & ***Improvement***):

- Monitor, Measure, Analyse, Evaluate
- Internal Audit
- Management Review
- Potential non-conformity & Preventive Action
- Non-conformity & Corrective Action
- Continual Improvement

Document all of the above as required

BCMS - **'CHECK** & **ACT'**

BC PROGRAMME MANAGEMENT

Note from Author / Owner of ***this*** Guideline Document

The user / reader is reminded that this guideline is 'approximately' based on ISO 22313 (ISO 22313:2020) - and that the author / owner has attempted to simplify / offer further explanation of the latter (in the many places where it is felt that this might be of benefit to the user / reader) - mainly in an attempt to provide a better understanding of 'what is required'

An example of where the latter (simplification / further explanation) might be needed concerns the generally historical use within the 'BC community' (and thus in ISO 22313) - of the term *'**understanding the organisation**'*

Originally used in the now defunct BC standard 'BS-25999' (a major reference source for the ***original*** development of ISO 22301 and ISO 22313), the actual meaning of this term was somewhat confusing and, in reality, mainly (but not exclusively) related to the conducting of two major component parts of any BC process - i.e. 'Business Impact Analysis' (BIA) and 'Risk Assessment' (RA)

Whilst it is correct to say that completing a BIA and RA (on an organisation) typically leads to a significant understanding of some ***parts*** of that organisation - there would certainly be additional work to do in other areas, to *thoroughly understand the organisation **as a whole***

Only by achieving the latter can effective, efficient and appropriate BC measures be introduced into an organisation e.g. without this thorough understanding, how would one know if the BIA and RA ***scopes*** had included all appropriate parts of an organisation in the first place?

ISO 22313:2012 had arguably taken a further step backwards on this matter by not only retaining the term 'understanding the organisation' - but also using it to additionally cover something known as the '***context***' of the organisation i.e.

'……………….**Understanding the Organisation and its *Context*** (ISO 22313:2020 / 4.1) - *by evaluating and understanding the external and internal issues (issues can include positive and negative factors / conditions for consideration) which are relevant to its purpose and operations - and accounted for when establishing, implementing, maintaining and improving its BCMS - and in assigning associated priorities……………………'*

For a (hopefully) better / clearer explanation of '**Understanding the Organisation**' *as a subject in its own right* - see Section 5 / 2 of ***this*** guideline document (starts page 119)

A stand-alone explanation related to the 'context' of the organisation can be found in ***this*** guideline document (**sub-section** 4 / 1.4 - starts page 69)

Deliberately Blank

Section **4 / 1** - **PLAN** - *(**PRE**-prepare)* for **how BMCS** should be **introduced into an organisation**

Reminder: See 'important note' - page 18 - it applies to ***all*** of this Section 4 / 1

Note 1 - section 4 / 1 refers to the necessary ***PRE-preparatory*** steps to be taken **BEFORE** a BCMS is actually introduced and becomes operational (is implemented) within an organisation

Note 2 - whilst use of the term '***BC programme management***' is used in ***this*** section 4 / 1 in a ***pre****-preparatory* context - note well that the term ***also*** applies equally throughout **ALL** of the subsequent sections of this guideline document, ***but*** then (in such subsequent sections) applying in a ***different*** context i.e. being one of ***continual*** on-going programme management - as it applies to all 'elements' of the ***entire*** BCMS programme management cycle

Note - the 'other elements' mentioned above & below will be covered later in this guideline

At the centre of the BCMS elements diagram (figure 3 / page 49) is an element known as 'BC Programme Management'. The latter refers (in the context of this Section 4 / 1 ***ONLY*** - see note 2 above) to the core management of the various ***projects*** - which require completion ***before*** moving on to the 'other BCMS elements'

These projects are collectively known herein as *a 'pre-preparatory programme'* - hence use of the term 'BC ***programme*** management', instead of the more commonly used term '***project*** management'. (However, as this 'programme' is effectively still a collection of individual projects, traditional project management tools and techniques [e.g. Gantt Charts, Pert Charts etc.] may still be used to map out and monitor the programme's progress, if so desired)

The projects for completion in this ***pre***-preparatory phase include (list is not exhaustive):

1. ***Originate & maintain*** appropriate ***documented material*** re the progress ***of each component project*** (can be used in subsequent audit to evidence compliance with 'whatever needs to be complied with') (ISO 22313 / 7.5 / Documented Information)

2. Research and document the ***requirements / reasons*** (BC influences / drivers) ***for introducing a BCMS*** e.g. more competitive; better resilience; more profitable; regulatory reasons; life or death etc. (see ***this*** document - pages 59 - 65)

3. Attain and retain ***buy-in***, ***leadership*** and ***on-going commitment / support*** (at least in principle for now) for the BCMS by / from the organisation's ***top management*** team (ISO 22313 / 5 / Leadership)

4. Identify, document and evaluate '***External and Internal BC Contexts***' - which are of a BC related relevance to the organisation (ISO 22313 / 4 / Context of Organisation)

5. Identify ***needs & expectations of stakeholders & other interested parties*** (ISO 22313 / 4.2 / Understanding Needs & Expectations of Stakeholders / [other Interested Parties]. [4.2.1 = 'General' & 4.2.2 = 'Legal and Regulatory])

6. * Take action to identify ***Risks & Opportunities*** which might be of 'interest'(ISO 22313 / 6.1 / Actions to address Risk and Opportunities)

7. Determine, establish and document ***BC Objectives & Planning** (for how) **to Achieve Them*** (ISO 22313 / 6.2 /BC Objectives)

8. Introduce an appropriate method re BCMS '***Change Planning***' (ISO 22313 / 6.3)

9. Establish and document the ***scope of the BCMS*** (ISO 22313 / 4.3 /Scope)

10. Set (establish) and document ***BC Policy*** (ISO 22313 / 5.2 / Policy)

11. ***Prepare plans to achieve what is required in this pre-preparatory programme phase*** (ISO 22313 / 6.2 / Plans to achieve BC Objectives [already included under 7. above])

* 'Risks & Opportunities' as documented in sub-clause (**6.1**) ***relate*** to the ***effectiveness*** of the BCMS

Risks ***related*** to ***disruption*** of the organisation's 'business' are different - and are addressed separately in ISO 22313 sub-clause (**8.2.3**) (**Risk Assessment**). To make this clear, sub-clauses 6.1 and 8.2.3 do not refer to the same thing

Note 1 - points 1 to 11 above are expanded upon (if / as required) starting on page 58

Note 2a - ***If*** the intent is to build a BCMS ***in full conformity with ISO 22301 requirements*** - the following must ***also*** be considered (ISO 22313 / 4.4 / 'Business Continuity Management System' refers):

Clause 4.4's purpose is to emphasise the need for the organisation to implement and maintain the appropriate ***PROCESSES necessary*** (including any associated interactions) for it to ***meet the BCMS requirements of*** ISO 22301:20XX (current version). In determining these processes (+ interactions etc.) and their application throughout the organisation, the following should be accounted for:

a. Research and identify the appropriate processes (accounting for associated 'risks and opportunities' as per ISO 22313 / 6.1)
b. Determine the inputs required of - and the outputs expected from - such processes
c. Determine the sequences, interactions & dependencies / inter-dependencies of such processes
d. Determine & apply the criteria and methods (including monitoring, measurements and related performance indicators) required to ensure effective operation and control of such processes

e. Determine and make available the associated resources required
f. Assign responsibilities, authorities etc. re training for, managing, operating etc. such processes
g. Evaluate such processes and implement any changes needed to ensure that they achieve / continue to achieve intended results
h. Continue to improve such processes where feasible / possible (thus improving the BCMS)

To the extent necessary, the organisation should:

I. Maintain documented info to support operation of its processes and supporting mechanisms

II. Retain such documented information

Note 2b - Regardless of the reason given (e. g. compliance with ISO 22301 requirements) for producing what is described above in 'note 2A' - it is recommended that ***the requirements of the latter should typically*** (but not always) ***be accomplished anyway*** by ***MOST*** organisations intending to 'produce' a BCMS - ***even if not formally intending to meet ISO*** 22301 ***requirements***

However, smaller / simpler / equivalent organisations (***not*** intending to meet ISO 22301 requirements) could (should?) adapt (simplify /modify) the 'note 2A' list (to suit their own circumstances) accordingly

4 / 1.1 - **Documented Records** relating to BC ***Pre-preparatory*** Programme Projects

Cross Reference - ISO 22313 / **Documented Information** / 7.5

It will be necessary to produce and maintain appropriately comprehensive reports, records and similar documentation - relating to ***most aspects of activities conducted for BCMS purposes*** etc. (One of the main reasons being 'evidence' of something having been done e.g. conformity to requirements, effective operation of a management system [via e.g. training; exercising, completion of business impact analysis etc.]. Such evidence is typically used for BCMS monitoring and evaluation purposes e.g. compliance [audit] checks)

Consequently, a fit for purpose 'controlled BCMS document system' must be established and maintained by the organisation - together with robust measures for the completion, retention, safeguarding and disposal (as required) of all such documentation, regardless of its 'medium' i.e. hard or soft copy

The organisation should specify generally acceptable formats (e.g. language, graphics) and medium (paper, electronic) used for the above purposes

Note that said 'document system' is also applicable to ***all*** BCMS ***pre-preparatory programme projects and similar*** (i.e. as per ***this*** Section 4.1)

Note - see Section 4 / 6 of this guideline document (page 113) for more on 'documentation'

4 / 1.2 - **Typical Influences** - 'Why should we introduce a BCMS into our Organisation?

Note - the above title reflects how such influences (also known as [BC] 'Drivers') might relate to an organisation's decision to introduce (or not) a BCMS

Cross Reference - ISO 22313 / **'Context'** / 4

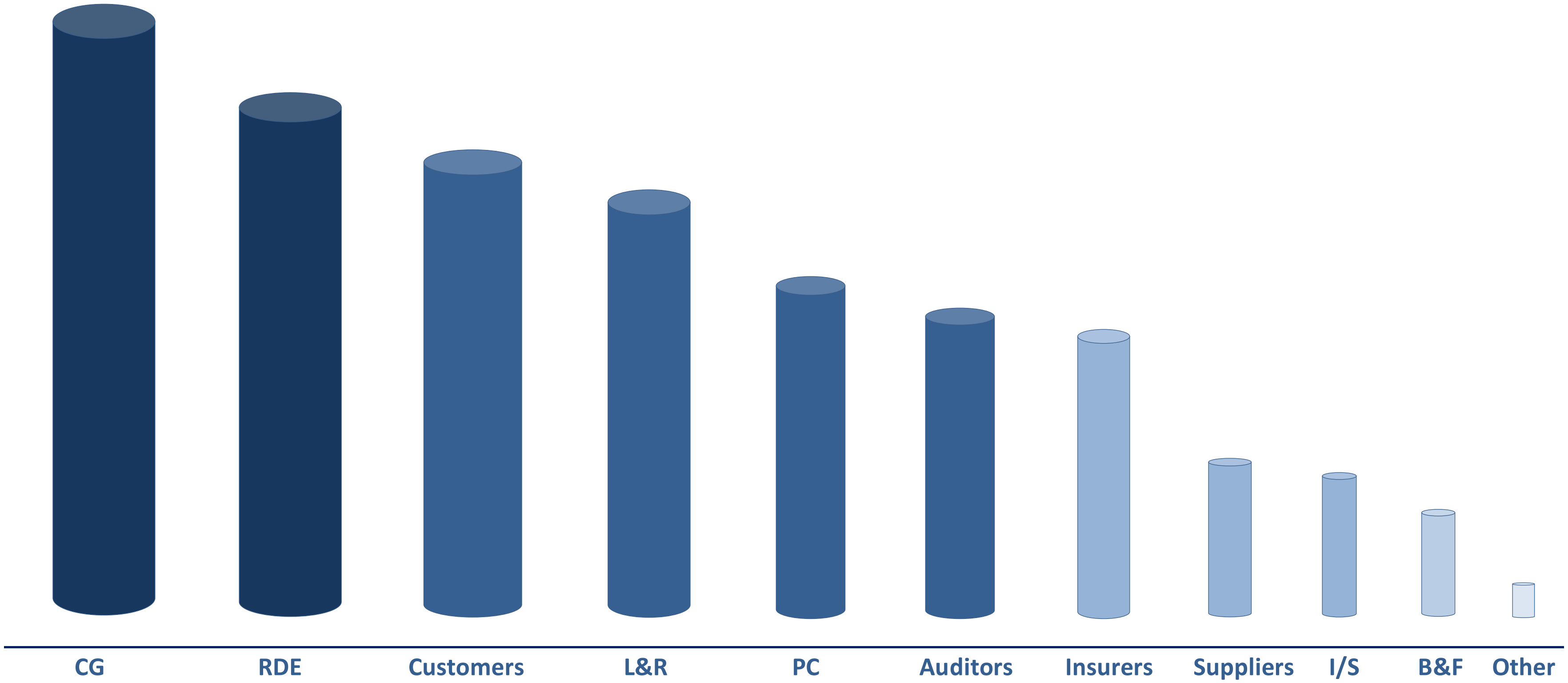
There are many influences (internal & external) related to why an organisation might want to introduce a BCMS

Figure 5 (next page) presents some of the more common influences (list is ***not*** exhaustive) - via a bar chart display of the comparative 'degree of influence' of each

These influences (and others) are expanded upon (in no particular order) via supporting text shown on pages 61 to 65. Some have been provided in an aviation context

The above were taken from an associated 2013 survey. They have been retained herein for comparison purposes with more current influences - as an example of how some (if not many) typically remain valid, despite the passage of time

What ***can*** (and does) change, however, is the comparative degree of influence of each such driver - together with the occasional 'disappearance' of some and the occasional 'appearance' of others (new ones)



CG = Corp. Governance; 'RDE' = Real Disruption Experience'; 'L&R' = Legal & Regulatory; 'PC' = Potential Customers; 'I/S' = Investors / Stakeholders; 'B&F' = Banks & Finance

Figure 5 - Some Typical External Influences / Drivers (2013) - re Introducing BCMS into an Organisation (Source & © - Chartered Management Institute 2013)

More Info re BC Influences / Drivers - in no particular order

Reminder - without ‘**risk**’ (or more correctly, the ***threats*** and associated ***vulnerabilities*** which give rise to ***risk***) there would obviously be no need for business continuity (or ‘risk management’ for that matter)

Supply Chain - a significant BC related issue for many organisations is reliance on key suppliers

Fuel, catering, flight despatch services, passenger and ramp services, engineering support etc. - are some of the many dependencies which ***airlines*** might have on external suppliers. Even if an airline is able to operate many of such services itself - it is always open to some risk e.g. fuel supply is largely outside the direct control of any airline (a similar argument applies to airports)

At ***airports*** - supply services such as catering, security, ground handling, utilities, de-icing stocks, duty free outlet stocks etc. - may require similar considerations. Some airports even contract out their air traffic services to third party providers

Supply chains invariably involve people - yet another area of vulnerability e.g. industrial action; sickness (pandemic), terrorism etc.

As a result, organisations /customers (airlines, airports etc. in the context used here) are increasingly putting pressure on their supply chains to themselves adopt BC techniques / programmes - to better ensure continuity of supply

This task would obviously be much more effective and efficient for all concerned if a common, universal BC standard was adopted e.g. ISO 22301 / ISO 22313 would be the logical choice - even if used as a guideline rather than for the more complex ‘certification’ process

Some supply organisation standard practices can exacerbate potential business continuity problems - notably:

- Adoption of ‘lean (just-in-time) practices’
- Globalisation of supply chains
- Focused factories and centralised distribution
- Outsourcing
- Reduction in the number of supplier base facilities
- Volatility of demand
- Lack of transparency and control procedures etc.

Investors & other Appropriate Stakeholders - will wish to see that their investments and / or interests are safeguarded - and one of many ‘tools’ available to an organisation for doing so is to ensure that ‘continuity’ is built into associated business plans

It is possible (desirable in appropriate circumstances) for investors to force this issue (e.g. via shareholders meetings) if an organisation is reluctant to take ‘business continuity steps’ itself

Auditors - external / internal auditors will often look for a BC Programme to be in place for a variety of reasons e.g. legal, regulatory, best practice, brand, image & reputation related matters, supply chain resilience etc. They will also typically seek evidence (compliance) that everything that supports such BC Programme is in place - and is continually maintained, trained, exercised, monitored, reviewed etc. - in an effort to achieve continual improvement

Potential & Existing Customers - a major factor in attracting potential customers (and retaining existing customers) is their 'reasonable' expectation that, during disruption, an airline will retain (to a 'reasonable' degree) its ability to fly and an airport its ability to continue associated operations. If there is no such reasonable certainty, customers might look instead to airlines / airports where there is

For example, airports which gain a reputation for maintaining and / or quickly recovering operations e.g. in snow and ice conditions or quickly clearing backlogs of flights after significant operational disruption (in conjunction with aircraft operators, ground handlers etc.) - will typically be preferred (by customers [actual & potential]), to those that do not or cannot

Example

British Airways (BA) cabin crew voted to take major industrial action in the period immediately before, during and just after the Christmas & New Year holiday period 2009 / 10, threatening severe disruption to tens of thousands of BA's customers. The reason for the strike was related to actions which BA management proposed taking to reduce the effects of the (then current) severe financial crisis, caused by the associated worldwide recession

BA's initial 'business continuity plan' was to take the cabin crew union to court (legal action) in order to prevent the proposed strike. The airline won on a legal technicality and the strike was temporarily abandoned - thus buying the airline a little more 'preparation time'

By mid-March 2010 the cabin crew union did actually strike (as the previous legal ruling preventing same had now been overcome by the Union). However, in the intervening period BA had trained some 1000 'other' staff (including some pilots) as temporary cabin crew and had also made arrangements to operate around 25 wet leased aircraft on BA services. The result was that around 60 - 65% of BA flights operated as normal during that strike

Further & longer strikes occurred during May / June but the airline was then able to operate up to 70% of its services due to the increasingly effective BC measures documented above

BA was lucky to have gained the 10 week 'window' in which to prepare its BC response. However, industrial action by BA cabin crew was a well-known historic ***RISK*** for which the appropriate 'risk / BC solutions' ***SHOULD*** have been better ***PRE***-prepared by the airline

Financial / Economic / Banking etc. - although not rated highly as an influence in Fig 5, the economic influences of the world-wide financial recession (as at 2012 / 2013) were actually having a significant influence as to whether organisations (in general) wished to 'invest' in areas of '***notional / potential***' worth rather than '***actual / real***' worth. The former includes business continuity i.e. BC is an intangible (***potential***) asset - but an asset nonetheless. (Update - the above situation still pertained [to a degree] as at early 2020 - not helped e.g. by other, associated factors such as the 2020 COVID-19 influenza pandemic)

Political / Legislative / Regulatory

Note 1 - Legislation typically 'makes' laws. Regulation typically ensures implementation and enforcement of laws

Note 2 - 'Political / Legislative / Regulatory' can apply at international and / or national and / or regional and / or local levels

Legal and regulatory requirement for the introduction of BC type techniques / programmes / management systems etc. by specified organisations, is becoming increasingly common and high profile, typically as related to the '***protection / safety of the customer***'; of the '***general community***' etc.

Increasing political interest is also becoming more significant (e.g. the UK Government applied due pressure on the parties involved - to resolve the BA example shown on the previous page)

Example

The UK's '**Civil Contingencies Act 2004**' (this is a UK law) requires e.g. that:

National emergency services (Police / Fire / Ambulance [Civil Defence] etc.)

National and Local authorities (State / Regional / County / Local / City and so on)

Nominated transport infrastructure such as ***airports***, rail and maritime etc.

Have effective ***BC measures*** in place - in order that they may continue to carry out their legally required [statutory] functions in response to a major disruption event

(Paradoxically, strangely, illogically and unfortunately - UK [and all other] ***airlines*** *are* **NOT** *directly subject to this law.* ***Trains*** *- yes;* ***ships*** *- yes;* ***airports*** *- yes;* ***airlines*****........................no***!!!!!!!)*

Additionally, ***local*** government authorities are similarly responsible for promoting BC to appropriate business and voluntary bodies within their spheres of influence / local areas - in support of a 'resilient community' concept. In this case, airlines ***are*** included

Insurers - Insurance cover for business disruption risks has for long been seen by many organisations as a relatively simple way of getting around ***some*** aspects of the 'BC problem' (i.e. by '*transferring*' the ***risk*** to the insurer) - albeit at a cost (i.e. increased insurance premiums; greater insurance excesses; reduced insurance coverage etc.) - and the disruption will happen anyway (if it is going to happen) - regardless

Insurance companies in general are now more pro-actively looking for evidence that effective client operated BC techniques / programmes / solutions etc. are in place in order to reduce their own risk of exposure. If this evidence is not available, it is logical (and reasonable) for the insurance companies not to cover the risk - or to cover the risk at an increased premium and / or by imposing greater excesses on the organisation etc.

External & Internal Changes, Trends, Influences etc. - which impact (for real or potentially) on the business e.g. global warming (= more adverse weather conditions such as hurricanes; 'bushfires'); terrorism; communicable disease (pandemic); cyber-crime etc.

Corporate Governance - was probably the most significant area (at least it was in in 2013 [by 2020 this had changed to 'technical concerns' {typically ICT related} + 'cyber' related threats and data breaches]) influencing general implementation of BC measures - and comprised both internal and external influences - an example of the latter being investors / shareholders

Competitive Advantage - a significant influencing factor in the private sector

Internal Factors - e.g. (list is not exhaustive)

- Nature of the organisation's business (suitable for BCMS introduction?)
- Adequate capabilities (including resources [esp. finance / budget], knowledge & competencies) to support BCMS introduction?
- Prospects of top management 'buy-in'?
- Prospects of staff buy-in / voluntary support (including perceptions, culture, union influences etc.)?
- Potential to establish required BCMS infrastructure - conceptually & physically?

Standards / Reference Models / Guidelines / Templates / Best Practice etc. - e.g. certification to an appropriate standard (such as ISO 22301) and / or similar (e.g. self-declaration of alignment with ISO 22313) - ***may*** result in potential advantages (including competitive / financial and reputational) to an organisation - over and above the direct & more obvious BC 'spin-offs'

Time Factor - is an increasingly significant influence as 'modern' expectations demand almost instant fulfilment

For example, if an airline's website and / or call / contact (reservations) centre and / or social media capability is not quickly and easily available (for whatever reason) - actual and potential customers might rapidly look for solutions to their expectations elsewhere - especially as the 'old' concept of customer loyalty is now almost non-existent

Actual Experience - of a major disruption event(s) & the need to apply the recommendations of associated 'lessons learned'

- e.g. the 2010 volcanic ash disruption in Europe which had (extreme) adverse effects on airlines and airports operating in the region + associated 'knock-on' effects worldwide
- e.g. the swine flu pandemic of 2009/10 - and its effects on aviation + lessons learned for when (at some future time) e.g. the much more lethal 'bird (avian) flu 'goes pandemic'. Same goes for the 2020 COVID-19 influenza pandemic which had significant, adverse implications for airlines, airports etc.

Other Interested Parties - if not already included above - e.g. the general public; the media; trade and professional bodies; pressure groups (such as 'environmentalists') etc.

Note 1 - A reminder that the above list (pages 61 to 65) is far from being exhaustive i.e. it is representative only. The 'interested' reader could no doubt come up with significantly more influences / drivers

Note 2 - The above list slants heavily towards the private sector (in contrast with the public sector). Note that the public sector will have its own, unique BC accountabilities (many related to associated legislation, regulation, best practice etc.) - in addition to some of those already listed above

4 / 1.3 - Top (and other) Management Commitment

Cross Reference - ISO 22313 / **Leadership** / 5.1 to 5.3

Without unconditional, * demonstrable and on-going ***top management*** (TM) leadership, commitment and support etc. of / to the planned introduction of a BCMS into an organisation - the latter endeavour is likely to fail. However, it is illogical that such endeavour would even commence without such commitment and support having already been established

* For example - by ensuring that requirements are met, communicating the importance of the BCMS, approving associated finances / budgets, promoting continual improvement, supporting other relevant (BCMS) management roles etc.

Such leadership, commitment & support should be provided throughout the complete programme management 'life-cycle' of a BCMS (i.e. it should be ever on-going whilst the associated BCMS exists)

All ***other*** levels of the management team should ***likewise demonstrate*** appropriate leadership and commitment (re their capacity, capability and willingness) to fulfil applicable business continuity policy, objectives, roles & responsibilities etc. - related to their associated accountabilities

Such 'demonstration' may typically be achieved using e.g. a mix of direction, delegation, involvement, motivation, engagement, empowerment, co-operation, enabling (and participating in) achievement and retention of associated competencies, supporting (and participating in) associated exercise programmes etc.

(Unless the BCMS 'introduction proposal' originated with TM) the typical route followed is that of an appropriate subject matter expert within the organisation (e.g. usually from the Risk Management business unit; the Emergency / Crisis Response business unit; the Quality business unit; the Insurance business unit etc.) proposing same to TM, preferably accompanied by a pre-prepared, outline business case (tentative proposal)

Assuming provisional TM agreement with the latter, it is typically then presented to the organisation's board of directors (or equivalent) for discussion, with a view to their agreement also. Assuming that this is achieved, 'initial work should be able to commence'

At this very early stage in 'BC programme management' - two more factors need to be considered and acted upon by top management:

1. ***Each Director*** (or equivalent title / grade / role / position) should ***provide an outline brief to his / her own management team(s)*** on all of the above - and enlist (direct if necessary) their full commitment and support for same

2. The ***TM should appoint an appropriate Director*** or equivalent (known herein as the *'Top Management **BC Champion**'*) ***to provide strategic, top management oversight responsibility of the entire*** (pending) ***BC introduction task*** - from start to finish, and on-going thereafter - and as typically related to the programme management 'life-cycle' of the implemented BCMS

Where necessary, an appropriately constituted ***'steering committee'*** may also be appointed to support the 'BC Champion' and to provide guidance and support to the organisation's 'BC Manager' - when appointed

Evidence / demonstration of top management (and, where appropriate, line management etc.) commitment to appropriate aspects of the BCMS - might typically be provided by (list is not exhaustive):

- ***Appointing a BC subject expert(s) / specialist(s)*** (having appropriate authority, competency and experience) - to be responsible for the introduction / implementation project of the BCMS and (thereafter) for its effective and efficient day to day operation i.e. appoint a ***'BC Manager'*** (ISO 22313 - 5.3)

  Note 1 - the term 'BC Manager' shall be used henceforth in ***this*** guideline document [i.e. the document you are now reading] with the same meaning as given immediately above

- Overseeing ***establishment and effective communication*** (to all concerned) of appropriate * ***BC Objectives & Policy*** - in line with organisation's 'purpose' (objectives, obligations and strategic direction) (ISO 22313 - 6.2 / 5.2 / 7.4)

  * Note - for more information on top management's responsibilities for defining '*BC **POLICY***' (in terms of an organisation's '*BC **OBJECTIVES***') - See pages **85** and **81** respectively

- Determining the ***scope*** of the BCMS (ISO 22313 - 4.3)

- ***Ensuring on-going compliance*** with relevant ***legal***, ***regulatory***, ***best practice*** and other appropriate requirements (ISO 22313 - 4.2.2)

- ***Overseeing establishment of all other*** (required) ***personnel authorities; roles / responsibilities / accountabilities; competencies, experience requirements etc.*** - necessary to effectively and efficiently manage the implementation and on-going management of the BCMS (ISO 22313 - 5.3 [take a look at Table 3 of the latter if you have access to it {provides examples of typical BCMS roles & responsibilities}])

- ***Overseeing on-going sourcing & provision of adequate resources*** (ISO 22313 - 7.1)

- ***Overseeing integration of BCMS processes into the organisation's established maintenance, performance evaluation, audit, management review etc. processes*** (ISO 22313 - 8.1.2 / 8.5.4 / 9.1 / 9.2 / 9.3)

- ***Overseeing & actively supporting the achievement of continual improvement*** ('Non-conformity and Corrective Action' [ISO 22313 - 10.1] + 'Continual Improvement' [ISO 22313 - 10.2])

- ***Operational involvement*** e.g. via BC champion, steering committees, management committees, departmental / business unit committees etc. (ISO 22313 - 5.3)

- Active ***participation*** and ***support*** in / for associated ***training*** / competence (ISO 22313 - 7.2) + ***awareness*** (ISO 22313 - 7.3) + ***exercising*** (ISO 22313 - 8.5) …………… and

- Inclusion of the ***BCMS*** as a ***permanent agenda item*** at scheduled ***top level & other*** appropriate ***management meetings*** (ISO 22313 - 5.1)

- Communicating ***importance of*** & ***conformance with*** organisation's BCMS

- Ensuring ***intended outcomes*** of BCMS are ***achieved***

Notes:

1. Nominated junior management and non-management representatives from appropriate (BCMS involved) departments and business units within the organisation (*required to form & operate '**Disruption Support Units** - **DSUs**' / see pages 100 - 104*) should ***additionally*** be required (where appropriate) to undertake ***associated*** roles, responsibilities & accountabilities re the pre-planning and implementation of the business continuity programme

   Thereafter, such ***DSU***s shall be similarly involved throughout the entire on-going *'life-cycle'* of operational BCMS programme management - including active participation in the organisation's response to actual disruption related events

   DSU staff shall acquire and retain the required levels of competence (training) and experience (exercising and / or involvement in real BC related incidents) as documented in the appropriate (associated) 'terms of reference'

   Furthermore, the above mentioned BC roles, responsibilities and accountabilities might be integrated into job descriptions and skill sets - the effectiveness of which may be enhanced e.g. by including same in the organisation's 'appraisal, reward and recognition' policy. Where the latter ***is*** enacted, it should also apply equally to all other staff involved with the BCMS

2. Where necessary, the organisation may enlist the services of external (third party) BC specialist professionals / experts to assist to the degree necessary, in any or all components of its BC Programme Management life cycle (including the preparatory / planning phase discussed here)

> For ***aviation*** related organisations, such BC specialist(s) should be ***100%*** conversant with the appropriate aviation background of relevance (e.g. airline; airport; ground handling operator; maintenance & repair organisation; flight-training school etc.)
>
> **Do not** engage such a 'specialist' with e.g. experience only in banking / finance; industrial production; ICT etc. nor those who might describe themselves as 'overall / general' BC experts - but again, who do not have the required (***aviation related***) background and experience

3. All BC programme authorities, roles, responsibilities, accountabilities and similar should be defined, documented and subject to regular competency, experience and compliance checks. Associated reports & records should be maintained and retained

4 / 1.4 - Identify & Evaluate '**External** & **Internal BC Contexts**' - relevant to the Organisation

Cross Reference - ISO 22313 /Understanding the Organisation and its '**Context**' / 4.1

Note 1: For more info related to ***'understanding the organisation'*** - see Section **5.2** of ***this*** guideline

Note 2: ISO 22313 / clause 4.1 concerns recommendations for understanding the context of the organisation ***in relation to the BCMS***. The ***separate*** recommendations for establishing and maintaining business continuity itself are addressed in ISO 22313 / clause 8.1

The organisation should identify, understand (the ***context*** of [relationships with]) and document ***external*** and ***internal*** * issues (which are relevant to / impact upon its operating purpose) and adequately ***evaluate*** and ***account*** for same (as required) with regards to establishing, implementing, maintaining, improving, reviewing and prioritising its BCMS

* Issues can include positive and negative factors and should also account for 'risk appetite'

Examples typically include:

Note: This subject has, to some extent, already been covered further above (starts page 59) under '*4 / 1.2 - **Typical BC Influences (Drivers)***'. Accordingly, some of these 'issues' may not be repeated below

Organisation's *EXTERNAL* Context

- 'External context' (as used herein) refers to the social / cultural / political / religious, technological, competitive, financial, natural, criminal, communications etc. environments - at all levels and in all geographical contexts (international, national, regional and local), as appropriate to the organisation's operating purpose.............for example (list in not exhaustive):
  - What ***social / cultural*** responsibilities does the organisation have to the '***community***' in which it operates? For example, employment, safety, communications, religion (and referring to the latter) use of female staff etc.

    How does the '***community***' ***view the organisation*** e.g. as beneficial, undesirable, as a threat etc.?
  - How dependent is the organisation upon ***technology***? Also, how might rapid technology ***change*** have an impact(s) on the organisation?
  - How susceptible is the organisation to '***cyber-crime***'?
  - How dependent is the organisation upon ***natural resources***?
  - How dependent is the organisation upon an ***external supply chain(s)***?
  - How strong is the national and local level influence of 'involved' ***trade unions***?

- ***Parent & subordinate organisation*** considerations? (as appropriate)

- Under what ***economic*** climate does / could the organisation operate? What is the attitude to debt amongst those funding the organisation? How strong are the economies of the countries in which and with whom the organisation trades - and what are the benefits / downsides of associated tax regimes?

- What are the ***ethics*** of trade / business? What is the public and media perception of the ethics of the organisation and its activities? Is corruption (internal and / or external) a significant factor?

- What is the ***political*** climate (at all levels and all locations) in which the organisation operates? Would a change of same possibly change attitudes (for good or bad) towards the organisation and its 'type of industry' sector(s)?

- What is the general ***security*** climate in which the organisation operates? For example, what is the risk of ***terrorism***, ***civil unrest*** etc?

- Which ***laws, regulations*** etc. apply and are they local, national, international?

- What ***environmental*** considerations need to be accounted for? What is the organisation's own impact on the environment e.g. pollution, noise?

- What external events could impact on the organisation ***from nature*** and / or from '***neighbours***' - such as seasonal weather extremes, volcanic ash clouds, local power supply failure, pandemic, criminal activity (other than terrorism / civil unrest)?

- What are the ***commercial*** / ***competition*** benefits and risks of providing the product / services / operations?

- What are the ***brand*** / ***image*** / ***reputational*** benefits and risks of providing the product / services / operations?

- ***Risk appetite / potential opportunities*** (external context)

- Consideration of the results of any existing ***Risk Assessments*** (or similar)

- Consideration of other inter-related ***external*** context issues *which **might** have already been identified and / or evaluated by other means - including use of **other** 'management systems'* (and similar) *which might already be in place within the organisation* e.g. risk management system; security management system; environmental management system; quality management system; information management system etc.

- Associated methods / types of ***external communications*** involved etc.

Organisation's INTERNAL Context

The (non-exhaustive and in no particular order) list below relates to an organisation's 'internal context' - as relevant:

- What the organisation 'does' (i.e. its key products / services / operations) - & who is / are the recipients (customers / clients / recipients) of same
- Corporate governance + organisational perceptions, values, culture etc.
- Business structure / model; decision making methods; prioritisations; other types of 'modern management systems' used (i.e. besides the proposed BCMS)
- Types of processes, procedures etc. constituting / forming / contributing to associated key main and key supporting activities
- Dependencies and relationships
- Organisation's operating location(s)
- Organisation's capabilities expressed in terms of available resources & knowledge
- Information (systems types [e.g. hard & soft copy]; flows / access; storage; security etc.)
- General awareness & commitment of / to BCMS in general
- General policies & objectives + how achieved / implemented etc.
- Risk appetite / potential opportunities (from an internal context viewpoint)
- Business ethics and similar - including internal standards, best practice etc.
- Staff loyalty / dedication / commitment
- Internal comms (what type; how managed, used, maintained etc.)
- Tentative future intentions / plans / opportunities etc.
- etc.

4 / 1.5 - Understanding the **Needs** & **Expectations** of **Stakeholders** / other '**Interested Parties**'

Cross Ref: - ISO 22313 / Understanding Needs and Expectations of **'Interested Parties** / 4.2

DEFINITION:

- **Stakeholder / Other Interested Parties Analysis**

  The above is a 'business tool' which can be a useful starting point in the essential '***understanding the organisation***' task - the latter being a very important (initial) requirement re introducing and implementing BCMS into an organisation

  This analysis simply requires a brainstorming session(s) (by the organisation concerned) to identify and document all possible stakeholders / other interested parties associated / concerned in some valid way, with said organisation's capability to maintain 'continuity of operation(s)' - whatever the latter might be

  The results are placed in an initial ***order of importance*** (relative to what [needs & requirements] they [stakeholders etc.] are believed to ***expect*** from the organisation and vice versa - such expectations being listed alongside the associated stakeholder / interested party concerned)

  This initial list is then used to assess the adverse impact of a disruption on such expectations and, if necessary, the order of importance of the initial list revised

  Finally (and the main reason for this analysis) the information acquired is used to ***ASSIST*** in ***identifying*** and ***prioritising*** (i.e. 'scoring' by degree of urgency with regard to continuity of operations) the organisations **key products / services / operations** etc. (together with associated key main and key supporting activities [+ associated processes, procedures etc.] + their inter-relationships, inter-dependencies, resource requirements, subordinate procedures etc.)

Note - sub-clause 4.2 of ISO 22313 (2020 version) cannot be reproduced directly here due copyright restrictions. However, the following provides a summary of what is documented therein. If possible (desirable but not essential), also see ISO 22313 itself for the actual / full text:

General (4.2.1)

All organisations have stakeholders / other interested parties. Figure **6** (see page 75) provides an indication only of some typical candidates for the larger and / or more complex organisation

Concerning the establishment / implementation / operation of a BCMS - the organisation should identify all stakeholders / other interested parties having a 'stake' / interest' in such an undertaking - and then (based on their actual and / or potential **needs** and expectations re the BCMS) obtain and document their associated **requirements** - as they relate to the organisation (see example template - page 76)

When referring to 'associated requirements', the context relates to both 'de facto' (actual) and implied requirements - and also to how such requirements can be met by the organisation - depending on predicted / actual circumstances prevailing (an actual example of the latter is given in ISO 22313 - sub-clause 4.2.1 - last paragraph)

Legal & Regulatory (4.2.2)

An organisation should (when establishing, implementing and operating a BCMS) adequately account for all legal, regulatory and similar requirements (implied, stated, obligatory etc.) which are applicable to itself and to associated stakeholders / other interested parties (ISO 22313 is written on the basis that the organisation is aware of such requirements - this might not be the case in reality. The organisation is responsible [to the greatest extent possible] for ensuring that the latter does not occur / is minimised)

The information regarding such requirements should be documented and reliably communicated both internally and externally (for the latter this means all appropriate stakeholders / other interested parties). It should also be regularly reviewed and maintained

The organisation should reliably demonstrate that it has ready access to current and pending legal and regulatory requirements applicable to it - at the locations in / to which it operates - and should also document how it can meet such requirements. Said requirements might e.g. relate to:

- ***Emergency*** / ***Crisis*** / ***Incident*** etc. planning / management / response etc. (see associated definitions in the ***glossary*** of [separate document] CRPM Part 3 / Volume **1**)
- ***Business Continuit***y type matters
- ***Risk*** Management considerations
- ***Hazards*** / *threats* / *vulnerabilities* (e.g. storage and transport of dangerous goods by air) - and
- Anything else of relevance to the organisation

An organisation should also account for other requirements to which it subscribes (e.g. international & national standards; best practice; codes of conduct; professional body membership requirements etc.) - and, where appropriate, relate same to the needs / requirements etc. of stakeholders / other interested parties

Organisations operating in multiple locations may need to satisfy requirements of different jurisdictions. Where appropriate, the 'international dimension' must be considered here. ***This*** (obviously) ***particularly applies to* aircraft operators *flying international routes***

More Information

Having identified (and documented) stakeholders / other interested parties (as already described further above) we have seen that it is then necessary to obtain and document their associated requirements as they relate to the organisation. Examples of such requirements might typically include (list is obviously not exhaustive):

- ***Shareholders*** - requiring a return on investment and also having an interest in the 'viability' of the organisation 'to continue operations'

- ***Customers*** - requiring contractual conditions to be met; good customer service to be delivered; safety requirements (where appropriate) to be observed etc. e.g. for an airline customer all of these (and more) are 'customer needs'. (By selling an airline ticket the airline actually enters into a contract with the passenger / customer)

- ***Legislators*** and ***Regulators*** feature heavily in aviation related operations. Their requirements not only need to be accounted for - but **must** typically be met without fail

- ***All those who must be 'communicated with'*** as part of a typical airline / airport / GHA etc. operation have related requirements. Such parties range from airline / airport / GHA staff (internal communications) to customers, the media, legislators and regulators, suppliers etc. (external communications)

  For example, following a major ***aircraft accident***, survivors and the associated families, relatives and friends of all of the accident victims (alive or dead for latter) should be able to expect effective, efficient and expedient communications (crisis communications) with (from / to) the airline / airport / GHA / emergency services / appropriate government (all levels) agencies etc. involved

  Today this must include effective, efficient and expedient use of social media

Reminder

Organisations operating in ***multiple***, geo-political locations will need to satisfy the requirements of all the ***differing*** legal, quasi legal, regulatory and similar jurisdictions, as appropriate

This is particularly applicable to many airlines *(aircraft operators)*

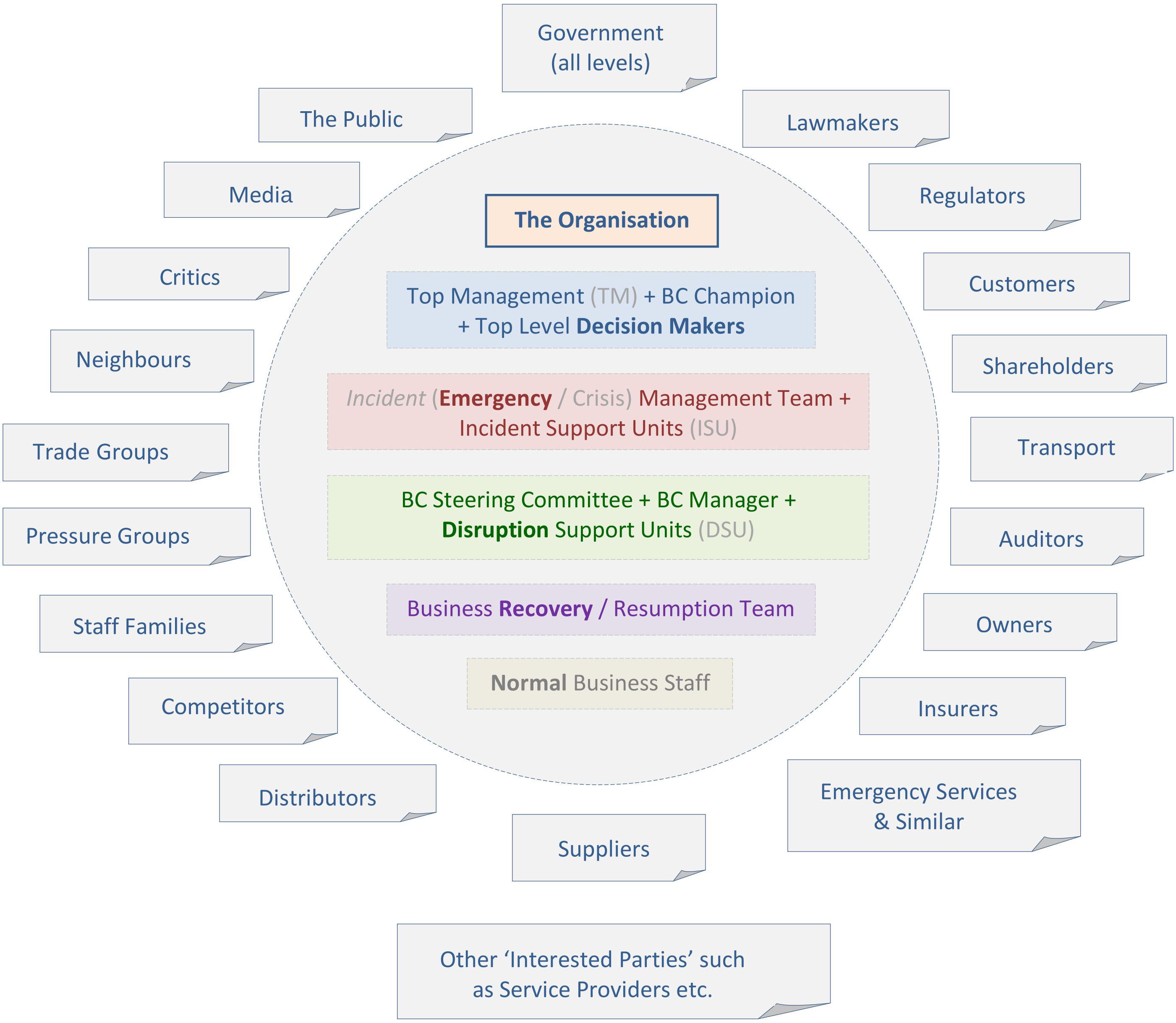

Government (all levels)
The Public
Lawmakers
Media
Regulators
The Organisation
Critics
Customers
Top Management (TM) + BC Champion + Top Level Decision Makers
Neighbours
Shareholders
Incident (Emergency / Crisis) Management Team + Incident Support Units (ISU)
Trade Groups
Transport
BC Steering Committee + BC Manager + Disruption Support Units (DSU)
Pressure Groups
Auditors
Business Recovery / Resumption Team
Staff Families
Owners
Normal Business Staff
Competitors
Insurers
Distributors
Emergency Services & Similar
Suppliers
Other 'Interested Parties' such as Service Providers etc.

Figure 6 - The ***Organisation*** + Typical ***Stakeholders*** / other ***Interested Parties***

Note 1 - above list is generic (and thus ***not*** exhaustive ***nor*** necessarily fully appropriate to an ***aviation*** related type situation) ……………… e.g. for ***airlines***, 'stakeholders / other interested parties' might typically include ***destination airports***; ***code-share / alliance partners***; ***ICAO***; ***IATA***; ***parent organisation***; ***subordinate*** (but independent) ***organisations*** e.g. cargo, in-flight catering, ground handling providers, travel & vacation service providers etc.

Note 2 - The organisation should establish the 'needs & expectation' of all stakeholders etc. (with regards to the organisation itself) - to determine their associated requirements - both obligatory and implied

Stakeholder / ***Other Interested Parties*** *Analysis* (***S*** / ***IP*** *Analysis)*

(Insert here Name [and / or Identity] + Type of Stakeholder / Other Interested Party)

- Detail briefly here what the particular S / IP does or 'is about' e.g. regulator; supplier; trade union; non-government organisation; pressure group etc.

- Detail briefly here the nature of the S / IP's relationship ***to*** / influence ***on*** / how influenced ***by*** - the organisation

- Detail briefly here ***actual*** and / or ***potential*** risks and / or benefits to the organisation as a result of this relationship / influence(s) with the S / IP

- Detail briefly here the ***actual*** and / or ***potential*** expectations of the S / IP (as related to and during normal operations by the organisation)

- Detail briefly here the ***actual*** and / or ***potential*** expectations of the S / IP during actual, disruption response operations by the organisation (i.e. for which BC measures applied by the organisation are expected to take the form of appropriate 'tactical BC solutions / treatment[s]' etc.)

- Apply a subjective grading / rating of importance (to the organisation) - of the S / IP's actual and / or potential relationship / influence e.g. '*high*, *medium* or *low*'

Example (above) - Typical ***Template*** for Recording Details of Stakeholders / Other Interested Parties

Note - a template such as the one above should be completed for ***each*** and ***every*** stakeholder / other interested party, identified as having some form of appropriate relationship with / having influence on / being influenced by - the organisation

4 / 1.6 - Actions to address **Risks & Opportunities**

Cross Reference - ISO 22313 / **Planning** / 6.1

Important Note: Sub-clause 6.1 (of ISO 22313:2020) (and use of the word 'Risks' [as used in the title above]) is related to the concept of '***risk appetite***' - the definition of which is shown below

- **Risk Appetite**

  The ***amount*** & ***type*** of risk that an organisation is broadly willing to pursue / retain (voluntarily accept / tolerate / be exposed to) ***at any particular point in time*** - with a view to attaining / maintaining / improving '***value***' (whatever the context of the term 'value' means to the organisation on a case by case basis) re its business objectives

  The use of risk appetite typically depends upon the mission, culture, policy and other factors which determine 'what an organisation is'; how it goes about its business etc.

  For example - **BC planning** is one (but ***only*** one) of several elements (treatments / controls etc.) of the ***Risk*** Management process, all such elements being designed to try to ensure that an organisation can continue to deliver its key products, services etc. to clients / customers etc. - when set against potential threats - which might (if realised) adversely impact on such delivery

  The depth of risk (including BC) planning and formulation of associated counter-measures etc. under consideration, typically depends upon the level of risk (per each considered threat) on the organisation which it (has typically [but not always] already considered) is prepared to accept - i.e. ***as predicated on its declared & current risk appetite***

  To develop this a little further (but with regards to the ***BC context only***), risk appetite can influence the organisation's 'calculations' of **MTPD**, **RTO** and **MBCO**. For example, the greater the risk appetite - the longer (relative / compared to the ***no*** / ***zero*** risk appetite situation) the RTO and MTPD timeframes might be **and** / **or** the lower the 'target level of continuity operations (MBCO / MAO) to be achieved by RTO'

  For example, procurement / allocation (***or not***) of required resources (to operate e.g. a BCMS) will be influenced by risk appetite

DO NOT confuse the meaning and use of the word 'Risks' (i.e. as used in 'Risks and Opportunities' as per ISO 22313:2020 sub-clause 6.1 at top of ***this*** page above) - with the '***other***' meaning of 'Risk', as defined in (separate document) CRPM Part 3 / Volume 1 (the associated meaning of same being commonly used throughout ***this*** CRPM Part 3 / Volume 2 guideline document - [which you are reading right now])

For the avoidance of doubt this 'other' meaning / definition is reproduced at top of next page:

- **Risk** (see also '*Threat*' and '*Vulnerabilities*')

  Evaluation of a specified ***threat*** (+ any associated ***vulnerabilities*** re what it is that is being 'threatened') to / on something / someone (the latter being subject to that threat) - which, when combined with the ***impact*** of that threat (on that something / someone) should it actually occur (be realised) - corresponds to the ***risk*** (with regards to that something / someone) - as related to / in the context of / with regards to that specified threat

  By its very nature such risk is neither precise nor scientific i.e. it is typically ***subjective***

  The considerations of any particular risk might (in appropriate circumstances) be influenced by any projected negative (adverse) & positive (beneficial) outcomes (see definition of 'Risk Appetite' - previous page) of potentially taking on that particular risk in the first place (assuming that there is a choice - sometimes there is not [e.g. an actual natural disaster occurrence])

  One (***but just one***) of several methods used to 'treat' (deal with) risk uses appropriate BC measures (e.g. via implementation of appropriate BC strategies & associated tactical solutions / treatments; via associated BC plans and procedures; via the setting-up and operation of Disruption Support Units [DSU] etc.)

The reader should note well that the 'Risks' we are referring to in this Guideline section ***'4.1.6' only*** - relate only to the definition shown on the ***previous*** page

Otherwise, use and context of the word 'Risk' as widely used elsewhere in this document (the one you are reading now) will typically be (instead) as per the definition at the top of ***this*** page. It is essential that the difference is clearly understood by the serious reader

Note 1: When updating the 2012 versions of ISOs 22301 / 22313 to the 2019 and 2020 versions respectively, the associated ISO 'technical committee' (which produced them) should have taken the opportunity to rewrite ISI 22313 / clause 6.1 so as to avoid the potential for the ambiguity and confusion just described above. That it did not do so is 'unfortunate' to say the least. **Note 2**: Unless intending to formally certify a BCMS to ISO 22301 requirements, many organisations (particularly 'smaller / simpler' organisations) can probably disregard what is written in this guideline document Section 4 / 1.6

Accordingly, we now provide valid comment just below (on 'Actions to address Risks & Opportunities') based ***only*** on the definition / concept of 'Risk Appetite' (as per ***previous*** page)

4 / 1.6 - Actions to address **Risks & Opportunities**

Cross Reference - ISO 22313 / **Planning** / 6.1

By identifying (determining) and beneficially (to itself) utilising appropriate 'risks and opportunities' (if any) the organisation ***might*** be better placed (regarding its BCMS) to:

- Achieve intended and avoid unintended outcomes
- Avoid / reduce undesirable factors / effects / consequences etc.
- Establish and maintain the desired degree of 'continual improvement'

It (the organisation) should also address the following, as appropriate (to be considered when planning and operating etc. the organisation's BCMS):

- Gain an understanding of, evaluate and appropriately utilise the results / outputs of complying with the requirements of ISO 22313's sub-clause ***4.1*** ('Understanding the Organisation and its Context') with regards to:

  - Better determination / management of identified ***risks*** and / or ***opportunities*** (i.e. risk appetite [being the amount and type of risks that the organisation might or might not consider])
  - Assignment of associated priorities
  - Any other matters requiring similar consideration

  The above should be conducted in the context of:

  - What the organisation 'does'
  - Its overall objectives
  - Its BCMS objectives
  - The degree and type(s) of 'risks & opportunities' under consideration

- Account for the general 'needs & expectations' of stakeholders / interested parties as per ISO 22313 sub-clause ***4.2.1*** - together with the application of relevant regulatory / legal requirements (stated / implied / obligatory etc.) as per ***4.2.2*** (i.e. documented; updated; communicated; safeguarded etc.) ………… including how they are to be met. This should include consideration of any associated 'risks and opportunities'

- Re the above, some examples of such considerations regarding their potential impact (beneficial or otherwise) on the BCMS might include:

  - The ability / competence (or not) of top management to 'top manage' - including ultimate 'management' (oversight) of the BCMS
  - Lack of required BCMS resources - including budget / funds
  - Lack of BCMS 'people' - i.e. numbers; competence; experience; motivation etc.
  - The ability (or not) of accessing new business where being a BCMS 'proficient and ready' organisation might be a major advantage etc.

- The organisation should also consider determining 'risks & opportunities' re:

  - Preventing unintended outcomes
  - Providing opportunities to improve the BCMS
  - Providing better process planning, implementation and controls re the establishment of the BCMS (as per ISO 22313 / clauses 6.1 and 8.1.1)

  …………….. and which ensures that:

  - Any 'risks and / or opportunities' taken are monitored for effectiveness as per ISO 22313 / 9.1 / 'Monitoring; Measurements; Analysis and Evaluation'

Deliberately Blank

4 / 1.7 - BCMS Objectives + *planning t*o achieve them

Cross Reference - ISO 22313 / **BCMS Objectives & Planning their Achievement** / 6.2

The organisation should establish and communicate its objectives re all major aspects of its BCMS project - being in line with its overall (general) objectives; identifying associated roles and responsibilities; setting appropriate targets for completion etc. Progress should be monitored, documented and, as the project evolves, reviewed and (as required) updated

BCMS objectives should typically specify e.g. (the below list is far from exhaustive):

- What will be done, why, by whom, when - and so on
- Resources required, including initial provision for associated budget
- Monitoring / evaluation of progress etc.

Within the BCMS context there are typically three types of 'objectives' (to consider, document, achieve etc.) i.e. strategic, tactical and operational. What we are concerned with here (in this ***pre-preparation*** phase of BCMS introduction) is the ***strategic*** element (the 'tactical' and 'operational' [doing] elements will be covered later in this guideline document)

BCMS *Strategic* Objectives

BCMS strategic objectives state the 'big picture' end purposes of what an organisation is aiming to achieve from the ***business continuity*** context / viewpoint - including (in ***very*** brief / general terms) how said end purposes are to be achieved. Such strategic objectives typically (but not always) form part of the overall BCMS ***policy*** statement

To check (on-going) that such objectives are / remain ***relevant*** and are being ***achieved*** it will be necessary (with regards to such objectives) to:

- Identify and assign associated responsibilities
- Set appropriate and realistic completion targets
- Regularly communicate them within the organisation and request associated feedback
- Measure them
- Monitor, review and update them (as required for latter)
- Document and retain them etc.

They should also:

- Be consistent with the organisation's BC policy (see page 85)
- Be clearly stated
- Be relevant and specific
- Be achievable

Examples of typical ***strategic*** BC objectives include:

- Implement and certificate (to ISO 22301 requirements) a BCMS system by (date)

- By (date) we shall implement a BCMS which is **a)** fully aligned with ISO 22313 **b)** adequately protects our key operations and **c)** meets stakeholders etc. requirements

- By (date) we shall be fully compliant with all national business continuity regulation
- During the next 12 months we shall improve our BC recovery time objectives (RTOs) by 50% whilst remaining within current budget constraints
- Over the next 2 years we shall target reduction of our insurance premiums by 15% as a result of introducing a BCMS fully aligned with ISO 22313

There are various methods of measuring achievement with regards to the above e.g.

- Actual certification to the ISO 22301 standard is itself a measure
- Feedback from associated exercises (testing) is another type of measure
- If you do get the 15% reduction in insurance premium (see examples of strategic BC objectives above - last bullet point) the objective's success has been measured

For more on *'measurement'* see Section 6 / 1 of ***thi***s guideline document - and also take a look at ISO 22313 itself (clause 9.1) - 'Monitoring, Measurement, Analysis and Evaluation'

For small to medium sized organisations (with no particular complexities) Strategic BC Objectives are typically documented as an inclusive part of 'BC Policy'. However, such objectives might be documented separately within BCMS documentation for the larger / more complex organisations - typically positioned just before the 'BCMS Policy' section

A suggested method of identifying strategic BC objectives is to look at your own 'wish list' of BC Outcomes (see page 42 for some typical suggestions of the latter) and then conduct a 'brainstorming' session(s) with appropriate parties - to come up with what is required. Remember that the latter should be stated in general terms only at this stage i.e. brief, amalgamated / consolidated and to the point, as per the typical examples shown above

As to who will be doing the brainstorming, the most likely candidates are the BC Manager; the top management BC champion and any associated BC steering committee / similar

TACTICAL BC objectives and associated ***plans*** etc. are covered herein in:

- **Section 4 / 3** (Establishing BC Awareness)
- **Section 4 / 4** (Establishing BC Competence)
- **Section 5 / 2** (Understanding the Organisation - BIA / RA etc.)
- **Section 5 / 4** (Incident Response Structure + Associated BC Plans & Procedures)
- **Section 5 / 5** (Maintaining & Exercising the BCMS)

OPERATIONAL BC objectives should be decided and documented separately by the organisation's '**Disruption Support Units** - **DSU**' themselves in their own (separate and specific) DSU BC plans (*as overseen by the organisations BC Manager / equivalent person*)

(For more information re **DSUs** see pages 100 [starting with title '**The Workers**'] to 104 - together with the appropriate sub-sections of **Section 5 / 4**)

4 / **1**.8 - Determine BCMS Scope Cross Reference - ISO 22313 / **Determining Scope** etc. / 4.3

It is important to ***determine*** and ***document*** what exactly the organisation's BCMS will and will not cover (its boundaries) - i.e. a BCMS ***scope*** is required. The latter is typically decided by the organisation itself. It will thus be necessary to establish the organisation's BCMS requirements before defining its scope (e.g. see '**Wish-list of BC Outcomes**' [***Requirements***] - page 42)

Consideration is also required re the organisation's missions / objectives / goals / obligations; its legal / regulatory requirements and environments; its obligations arising from internal and external contexts (including those of stakeholders / other interested parties [including employees / staff etc]); the scale / size of whatever it is that the BCMS is proposed to address …………… and how it (BCMS) fits into the organisation's overall business strategy (including overall ***risk*** strategy)

The 'scope' should also account for appropriate (relevant) matters as might be identified in ISOs 22313 - clause 4.1 and requirements arising from clause 4.2. (If not already included above and / or below)

Furthermore, the organisation might also need to consider the following (with regards to ***itself*** [list is not exhaustive]):

- Size; complexity etc.
- Location(s) where it operates; has influence etc.
- Key product(s) / service(s) / operation(s)
- Associated key main activities; key supporting activities; processes; procedures etc.
- Associated dependencies
- Associated resources
- Associated timescales
- Any operations / activities ***external*** to the organisation where desirable, permitted and possible / practicable to do e.g. an organisation's external supply chain etc.

……….. e.g. scope might ***include*** delivery of a specific product to a particular country/region only
……….. e.g. scope might ***exclude*** products of low value or which are no longer viable
……….. e.g. scope might ***exclude*** services which it is not obliged to provide
……….. e.g. scope might ***include*** only a sub-set of particular products, services etc.

From the 'scope' viewpoint, smaller / simpler organisations might consider applying BCMS to 'everything' from the outset - whilst this might be too ambitious (and possibly undesirable also) for the larger / more complex organisations - particularly if attempted 'all in one go'

For medium to large sized (and / or the more complex) organisations, the results of an * ***initial / exploratory*** Business Impact Analysis - BIA (see Glossary in [separate document] - CRPM Part 3 / Volume 1) might serve well to direct which ***potential*** areas of the organisation (including external aspects where appropriate e.g. external suppliers) might fall within the BCMS scope and in what priority order for addressing - with a phased approach possibly anticipated, perhaps spread out over several years

* Note - whilst **formal** BIA is covered later in this document (Section 5 / 2), there are several good reasons for performing this ***initial*** (exploratory [separate]) BIA during this BCMS ***pre**-preparatory* phase - one of which can be used to assist in deciding the ***INITIAL scope*** of the BCMS. In such circumstances, a follow-up (second / more in-depth / formal) BIA ***must*** eventually be conducted at the appropriate point in the BCMS implementation (**DO**) programme. The work already put into an ***initial*** BIA would not be wasted as it can form the foundation for this subsequent, ***formal*** BIA

Where an initial / exploratory BIA is ***not*** undertaken, an alternative might be to ‘brainstorm’ the matter - typically including inputs / debate from top management, middle management, subject matter experts (e.g. the BC Manager; external consultants), the BC champion, the BC steering group and other appropriate committees / persons etc. Such brainstorming etc. sessions might best be facilitated by the organisation’s BC manager / equivalent person

External input (e.g. regulators; suppliers; subject matter experts etc.) may also be required when considering ‘scope’ - depending on the nature of the organisation’s business

The BCMS scope **must** eventually include everything relevant to ongoing continuity of the organisation’s key product / services / ops - e.g. continuity of flight operations is obviously ***within*** every airline’s scope - whereas providing restaurant type facilities for staff might not be

Reminder - the ***nature*** of the organisation itself can dictate the BCMS scope e.g. charities and similar ‘not for profit’ (e.g. government) organisations may (will?) have quite different scope requirements from those of profit making organisations

Other scope considerations might include:

- ***Putting into context the scale of incidents that the BCMS will address*** (e.g. dealing with a **catastrophic aircraft accident** requires ‘hugely’ more planning, resources, training etc. - than dealing with a **serious aircraft incident**. Dealing with a **temporarily blocked runway** is a relatively straightforward - compared to **complete airport closure**)

- Identifying how the BCMS fits into the organisation’s ***risk management*** responsibilities - including any *risk appetite* considerations (see ISO 22313 / 6.1 [Addressing Risks & Opportunities] and 8.2.3 [Risk Assessment])

- Where part(s) of an organisation is / are excluded from the BCMS scope - the exclusion(s) should be documented (together with reason[s]). Potential exclusions should be thoroughly reviewed before being approved and documented. (Note: Where dependencies are identified in a BCMS they are obviously ‘in scope’ and thus cannot be excluded. Furthermore, exclusions are not ‘permitted’ if they affect the organisation’s ability to effectively and efficiently operate its BCMS - including e.g. all activities, resources, supply chain etc. required to deliver ‘in-scope’ product / services / operations etc.)

- If the BCMS is being integrated into an existing (different) management system, the organisation should ensure that all elements of the BCMS are included

- The BCMS scope is typically (but not always) included within an organisation’s BCMS ***policy*** document. It should be prepared in a manner / terms appropriate to the organisation’s size, nature and complexity - and reliably communicated to all appropriate stakeholders / interested parties

4 / 1.9 - Establish **BCMS Policy**

Cross Reference - ISO 22313 / **LEADERSHIP** / Policy - 5.2

Top management should demonstrate appropriate leadership and commitment

One (mandatory if certifying to ISO 22301 requirements) way of achieving this is to ensure that a ***BCMS Policy*** (compatible with the strategic [overall] direction of the organisation - amongst other matters) is researched, established, maintained, reviewed etc.

The policy should document the BCMS principles to which the organisation aspires and against which its performance might be measured. It should also include a ***high-level*** overview of the organisation's BC (**strategic**) objectives + its expectations, obligations, context etc. - in addition to serving as a useful interface 'tool' between top management and the 'BCMS' itself

The BCMS policy ***should*** / should be (with regards to the BCMS):

- Concise
- Provide a strategic indication of intention and direction
- Include a related scope
- Reflect the size, nature, complexity, extent etc. of the organisation
- Reflect the organisation's context (operating environment; culture etc.)
- Typically include strategic objectives (see page 81)
- Commit to satisfying appropriate requirements, obligations, commitments etc. - e.g. those which are statutory, legal, regulated etc.
- Identify and assign (within the organisation) the appropriate authorities / delegations / duties / responsibilities etc.
- Identify and include anything else that might be a significant consideration or compliance matter e.g. ISO 22301 et al - if certification to the latter is intended
- Reflect commitment to continual improvement

The BCMS policy ***may*** (with regards to the BCMS):

- Include a funding commitment
- Refer to related policies where appropriate
- Include commitments re implementation, competence, exercising, maintenance etc.
- Be integrated (as appropriate) with the policies of any other modern management systems in use by the organisation

Suitable provision should be made for approving the BCMS policy, retaining associated documented information, conducting periodic review and responding to any significant change to internal / external factors (e.g. to top management; re the introduction of new [and relevant / impacting] legislation etc.). The suitability of such provisions should relate e.g. to the size, complexity, nature and extent of the organisation (list is not exhaustive)

The contents of a BCMS policy should rarely change (provided, of course, that it is / was 'fit for purpose' in the first place)

The process of ***developing*** the BCMS Policy should consider:

- Formulating a definition of BCMS which is appropriate to the organisation's purpose (e.g. size, nature, complexity, culture, dependencies, operating environment(s), other contexts etc.) - as expressed in terms of its overall objectives and obligations
- Identifying the various components of the policy
- Identifying and committing to adherence of applicable laws, regulations and similar
- Identifying and referring to any 'good / best practice' guidelines available (including 'BC standards e.g. ISO 22301 / 22313') or e.g. other (external) organisations' BCMS policy documents - which might serve as an appropriate benchmark for what needs to be accomplished
- *Where applicable*, conducting a * '***gap analysis***' of any current or proposed BCMS policy within the organisation - compared with the benchmarks mentioned just above (+ any others not so mentioned [and as available] but which might also be of benefit)
- Developing the draft of a new (or revised) BCMS policy
- Reviewing the draft in order to ensure standardisation with other (related / appropriate) policy documents within or without the organisation (as applicable)
- Circulating draft policy ([internally & externally] - to appropriate parties) for review / feedback
- Amending the draft if necessary - to reflect the results of said review / feedback
- Agreeing and implementing 'sign off' of the policy with / by the top manager - and also gaining approval for how the policy is to be implemented (i.e. from a ***strategic*** viewpoint)
- Publishing / distributing the approved BC policy document
- Ensuring that the policy is carried out; complied with etc.

*** Gap Analysis**

A 'tool' used to assist an organisation to compare its ***actual*** performance (in a pre-defined area[s] of '*what it is that the organisation does*') with its ***potential*** performance. At its core are two questions:

"Where are we now?" .... and

"Where do we want to be at some stated, future time?"

If an organisation is e.g. not making the best use of its current resources; is foregoing investment in required capital or technology etc. - then it will probably be producing or performing at a level below its potential

A Gap Analysis should assist in identifying such deficiencies .... and more

A BCMS policy should include / ensure (list is not exhaustive):

- That it is available / maintained as 'documented information'
- The BCMS definition as formulated and referred to on the previous page
- Criteria (in very general terms) for the type and scale of threats, risks etc. to be addressed by the BCMS
- Appropriate details for how the policy is to be communicated and understood ***within*** the organisation and is to be made available (or otherwise - as decided by management) to ***external*** stakeholders / other interested parties
- Reference to any legislation, regulation, guideline, standard, principle, best practice, benchmark and other policy ***requirements*** to be complied with and / or considered
- A clear commitment to support all applicable requirements contained within the policy - including provision of funding and other appropriate resources
- The ***resources*** expected to be procured / allocated / assigned etc. (in ***very*** general terms)
- Details of all 'authorities' and / or 'delegations' required under the BCMS - including the person or persons responsible for managing the BCMS on a day to day basis

Note 1: - The top manager should appoint a Director / equivalent (known herein as the '***Top Management BC Champion***') to provide ***strategic***, top management oversight of the entire (***pending***) BC programme - from start to finish, and thereafter ***on-going***. The rationale and authority / delegation for this should be included in the BCMS ***Policy***

- Agreed scope of the BCMS - including limitations & exclusions
- Agreed BCMS strategic objectives (if not included separately)
- An ***objective*** setting framework related to ***establishment & maintenance*** of the BCMS
- An ***operational*** framework for the ***management*** of the BCMS programme - including a very brief overview of the roles & responsibilities of those charged with BCMS delivery
- The basis on which the policy is to be reviewed (e.g. by time; due to change etc.)
- The basis on how BCMS performance will be monitored / verified & measured
- An implementation and maintenance plan (strategy) for the policy
- A clear commitment to 'continual improvement' of the BCMS
- That the policy Is complementary to other applicable / relevant organisation policies (and also [possibly] to appropriate external policies)
- That the policy accords with the organisation's ***risk*** policy / strategy etc.

Other BCMS policy considerations might include:

- A (mandatory) requirement to establish BCMS within the organisation (e.g. as would typically apply to 'emergency services' such as Police, Ambulance, Fire & Rescue etc.)
- A glossary of ***key*** terms used in the policy
- A commitment to BCMS testing (exercising) and maintenance
- Anything else considered appropriate

Note 2: - An organisation's management team might not always be 'sensitive' to low probability, high impact risks - and even if they are, might want BC strategic and tactical solutions geared to their own specific interests rather than those of the organisation as a whole. This is where the **BC policy** comes in i.e. providing a central point of accountability for such managers - whilst reassuring them of a consistent and scoped approach to protecting **all** of the organisation's values (if within the scope of the BCMS), following a disruptive event - which requires a business continuity related solution(s)

Follow the links below to 'sample' different examples of some 'real life' BC Policy documents:

https://education.nsw.gov.au/policy-library/policies/business-continuity-management-policy

New South Wales Education / 2015

business-continuity-management-policy-pd-9010.pdf (lincs.police.uk)

Lincolnshire Police Force / July 2022 (due for review July 2024) - This 'policy' includes the following paragraph:

'………………..in relation to Business Continuity Management (BCM) the Force will adopt the principles described in ISO 22301- which specifies the requirements for a management system to protect against, reduce the likelihood of and ensure recovery from disruptive incidents……………….'

Business Continuity Policy (pwc.com.cy)

PWC / 2022

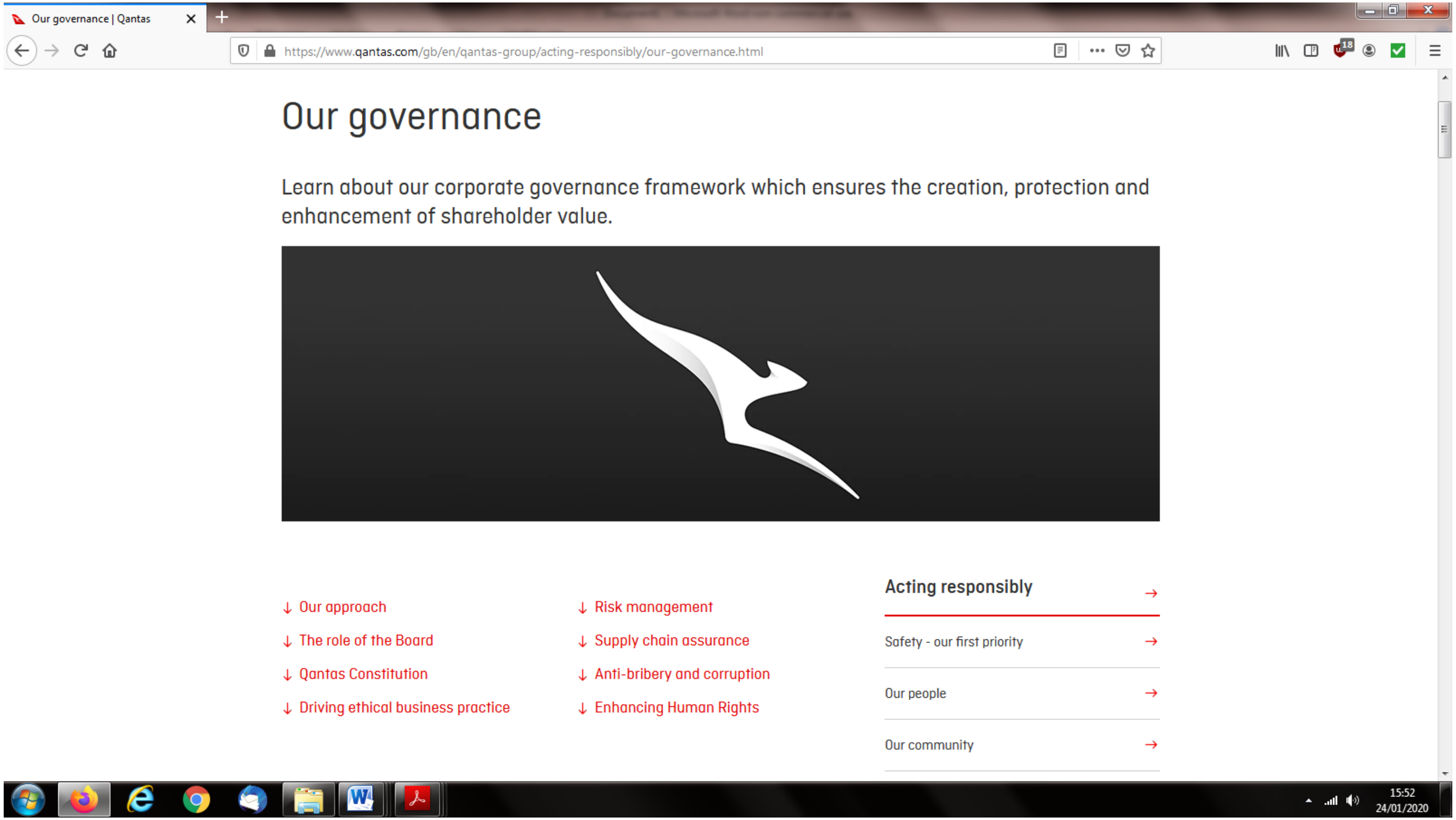
Following the link below immediately below should lead the reader to a completed 'sample / generic / template' BC Policy document. If (with the passing of time) the link ceases to work, a well performed internet search should find it again (or an appropriate equivalent):

https://issuu.com/public-it/docs/bcms-doc-05-1_business_continuity_p_34cc67391ed3c7

Note from Author / Owner of this guideline document (i.e. the one you are reading right now) - It has been difficult to find additional, 'linkable' examples of ***aviation*** related BC policies for airlines, airports, GHAs etc. - but they do exist (e.g. the 'Qantas Group ***Business Resilience*** Policy' - see next ***5*** pages for at least a small sample of aviation related material on this subject)

If anyone can assist in (legally & ethically) obtaining and forwarding (to said author / owner) any appropriate, additional links re the above subject area (i.e. Aviation Related Business Continuity Policy), they will be placed here as further examples. Contact details are:

info@aviation-erp.com


Our governance | Qantas
https://www.qantas.com/gb/en/qantas-group/acting-responsibly/our-governance.html
15:52
24/01/2020

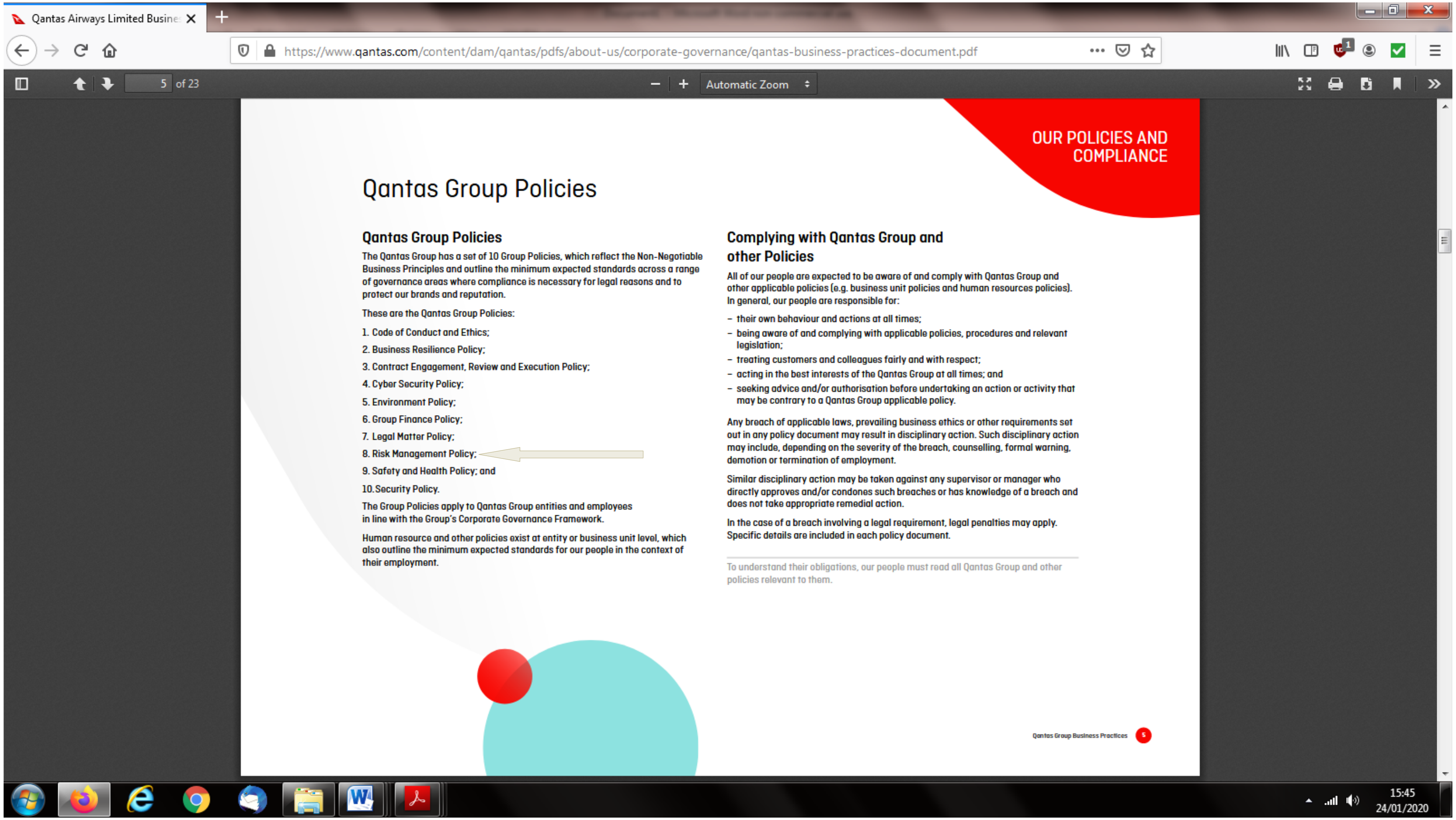
Our governance

Learn about our corporate governance framework which ensures the creation, protection and enhancement of shareholder value.

- ↓ Our approach
- ↓ The role of the Board
- ↓ Qantas Constitution
- ↓ Driving ethical business practice
- ↓ Risk management
- ↓ Supply chain assurance
- ↓ Anti-bribery and corruption
- ↓ Enhancing Human Rights

Acting responsibly →

- Safety - our first priority →
- Our people →
- Our community →


Qantas Airways Limited Busine
https://www.qantas.com/content/dam/qantas/pdfs/about-us/corporate-governance/qantas-business-practices-document.pdf
5 of 23
Automatic Zoom
15:45
24/01/2020

OUR POLICIES AND COMPLIANCE

Qantas Group Policies

Qantas Group Policies

The Qantas Group has a set of 10 Group Policies, which reflect the Non-Negotiable Business Principles and outline the minimum expected standards across a range of governance areas where compliance is necessary for legal reasons and to protect our brands and reputation.

These are the Qantas Group Policies:

1. Code of Conduct and Ethics;
2. Business Resilience Policy;
3. Contract Engagement, Review and Execution Policy;
4. Cyber Security Policy;
5. Environment Policy;
6. Group Finance Policy;
7. Legal Matter Policy;
8. Risk Management Policy;
9. Safety and Health Policy; and
10. Security Policy.

The Group Policies apply to Qantas Group entities and employees in line with the Group's Corporate Governance Framework.

Human resource and other policies exist at entity or business unit level, which also outline the minimum expected standards for our people in the context of their employment.

Complying with Qantas Group and other Policies

All of our people are expected to be aware of and comply with Qantas Group and other applicable policies (e.g. business unit policies and human resources policies). In general, our people are responsible for:

- their own behaviour and actions at all times;
- being aware of and complying with applicable policies, procedures and relevant legislation;
- treating customers and colleagues fairly and with respect;
- acting in the best interests of the Qantas Group at all times; and
- seeking advice and/or authorisation before undertaking an action or activity that may be contrary to a Qantas Group applicable policy.

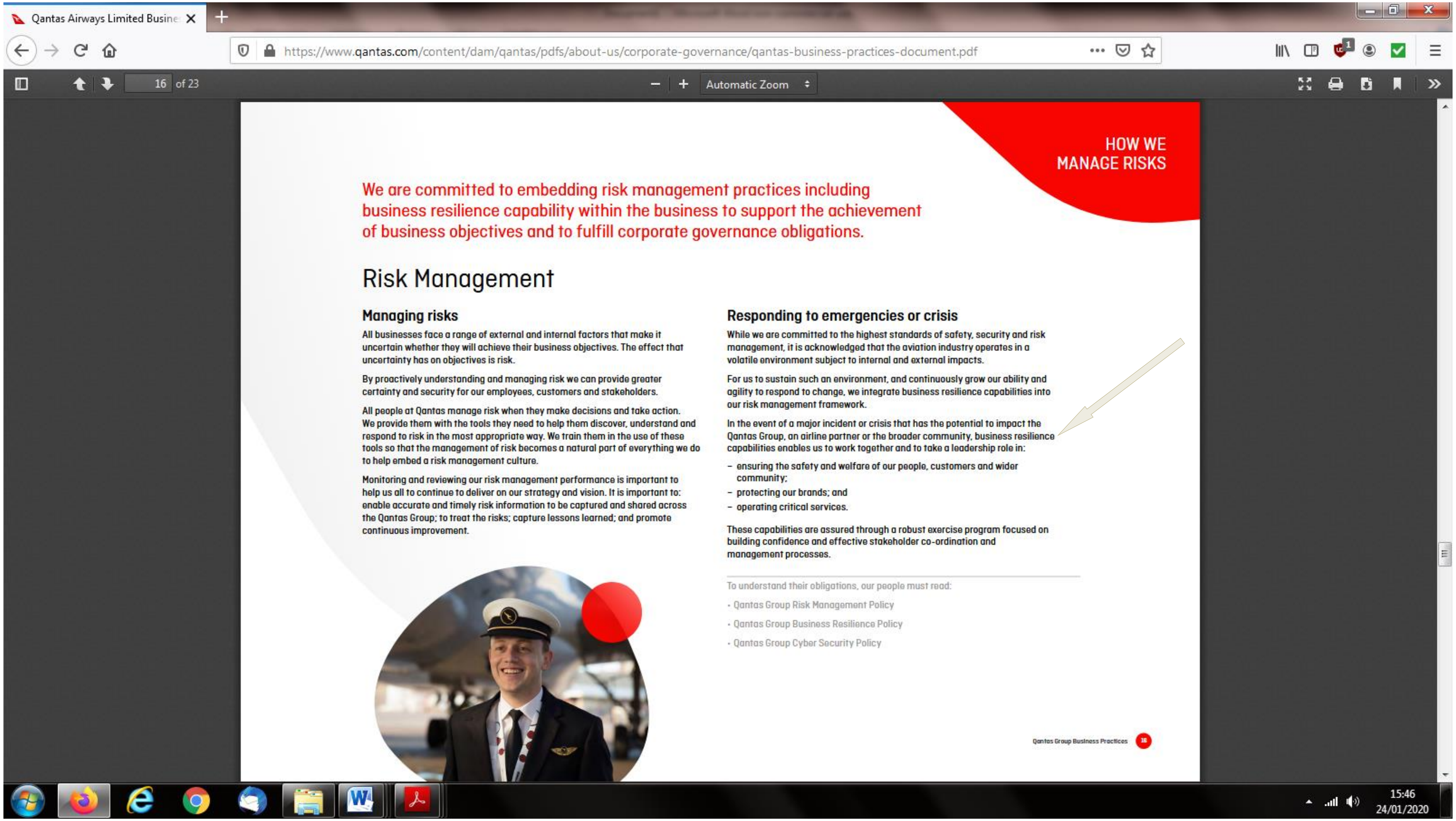
Any breach of applicable laws, prevailing business ethics or other requirements set out in any policy document may result in disciplinary action. Such disciplinary action may include, depending on the severity of the breach, counselling, formal warning, demotion or termination of employment.

Similar disciplinary action may be taken against any supervisor or manager who directly approves and/or condones such breaches or has knowledge of a breach and does not take appropriate remedial action.

In the case of a breach involving a legal requirement, legal penalties may apply. Specific details are included in each policy document.

To understand their obligations, our people must read all Qantas Group and other policies relevant to them.

Qantas Group Business Practices 5


Qantas Airways Limited Busine
https://www.qantas.com/content/dam/qantas/pdfs/about-us/corporate-governance/qantas-business-practices-document.pdf
16 of 23
Automatic Zoom
15:46
24/01/2020

HOW WE MANAGE RISKS

We are committed to embedding risk management practices including business resilience capability within the business to support the achievement of business objectives and to fulfill corporate governance obligations.

Risk Management

Managing risks

All businesses face a range of external and internal factors that make it uncertain whether they will achieve their business objectives. The effect that uncertainty has on objectives is risk.

By proactively understanding and managing risk we can provide greater certainty and security for our employees, customers and stakeholders.

All people at Qantas manage risk when they make decisions and take action. We provide them with the tools they need to help them discover, understand and respond to risk in the most appropriate way. We train them in the use of these tools so that the management of risk becomes a natural part of everything we do to help embed a risk management culture.

Monitoring and reviewing our risk management performance is important to help us all to continue to deliver on our strategy and vision. It is important to: enable accurate and timely risk information to be captured and shared across the Qantas Group; to treat the risks; capture lessons learned; and promote continuous improvement.

Responding to emergencies or crisis

While we are committed to the highest standards of safety, security and risk management, it is acknowledged that the aviation industry operates in a volatile environment subject to internal and external impacts.

For us to sustain such an environment, and continuously grow our ability and agility to respond to change, we integrate business resilience capabilities into our risk management framework.

In the event of a major incident or crisis that has the potential to impact the Qantas Group, an airline partner or the broader community, business resilience capabilities enables us to work together and to take a leadership role in:

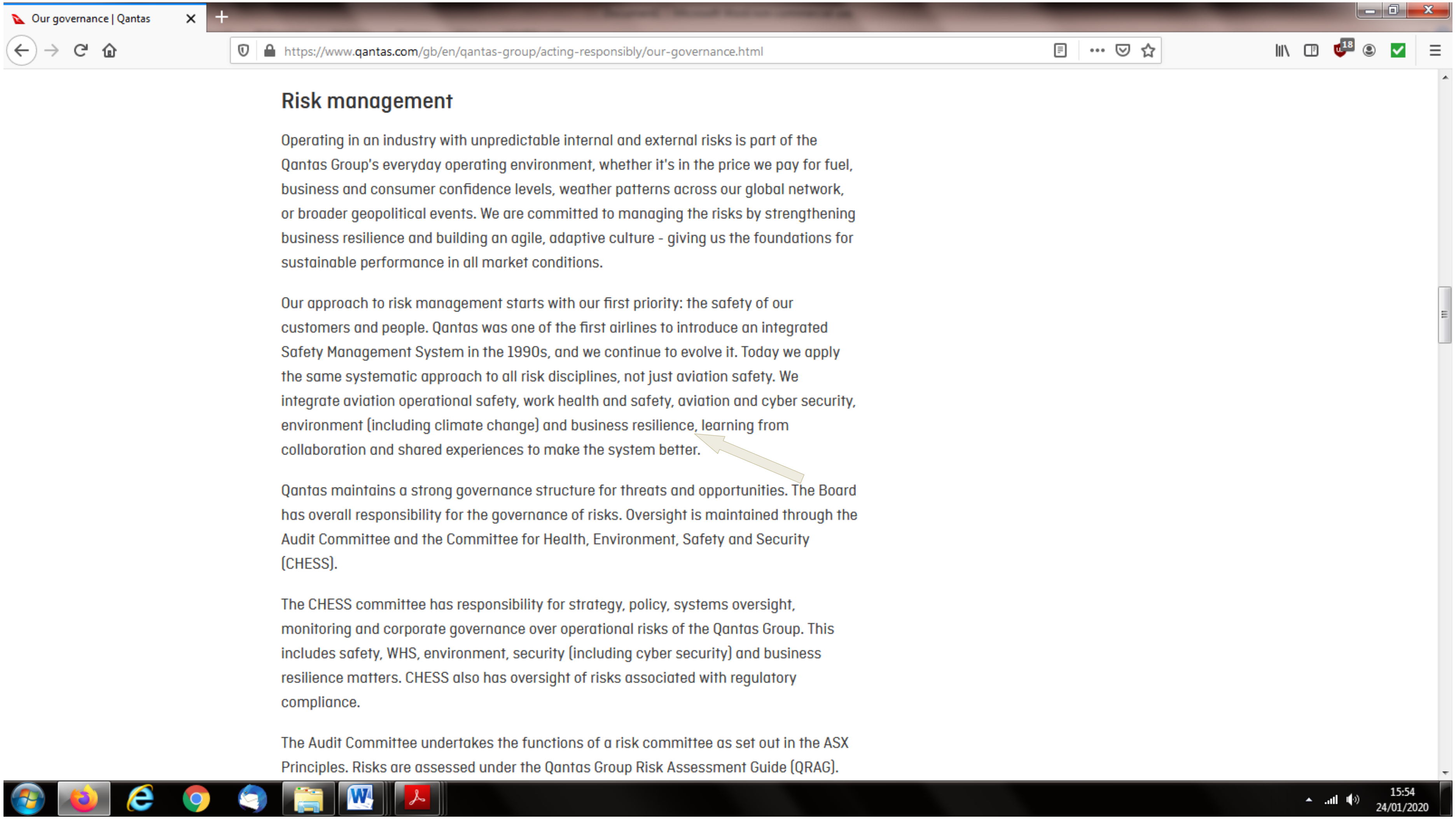
- ensuring the safety and welfare of our people, customers and wider community;
- protecting our brands; and
- operating critical services.

These capabilities are assured through a robust exercise program focused on building confidence and effective stakeholder co-ordination and management processes.

To understand their obligations, our people must read:

- Qantas Group Risk Management Policy
- Qantas Group Business Resilience Policy
- Qantas Group Cyber Security Policy

Qantas Group Business Practices


Our governance | Qantas
https://www.qantas.com/gb/en/qantas-group/acting-responsibly/our-governance.html
15:54
24/01/2020

Risk management

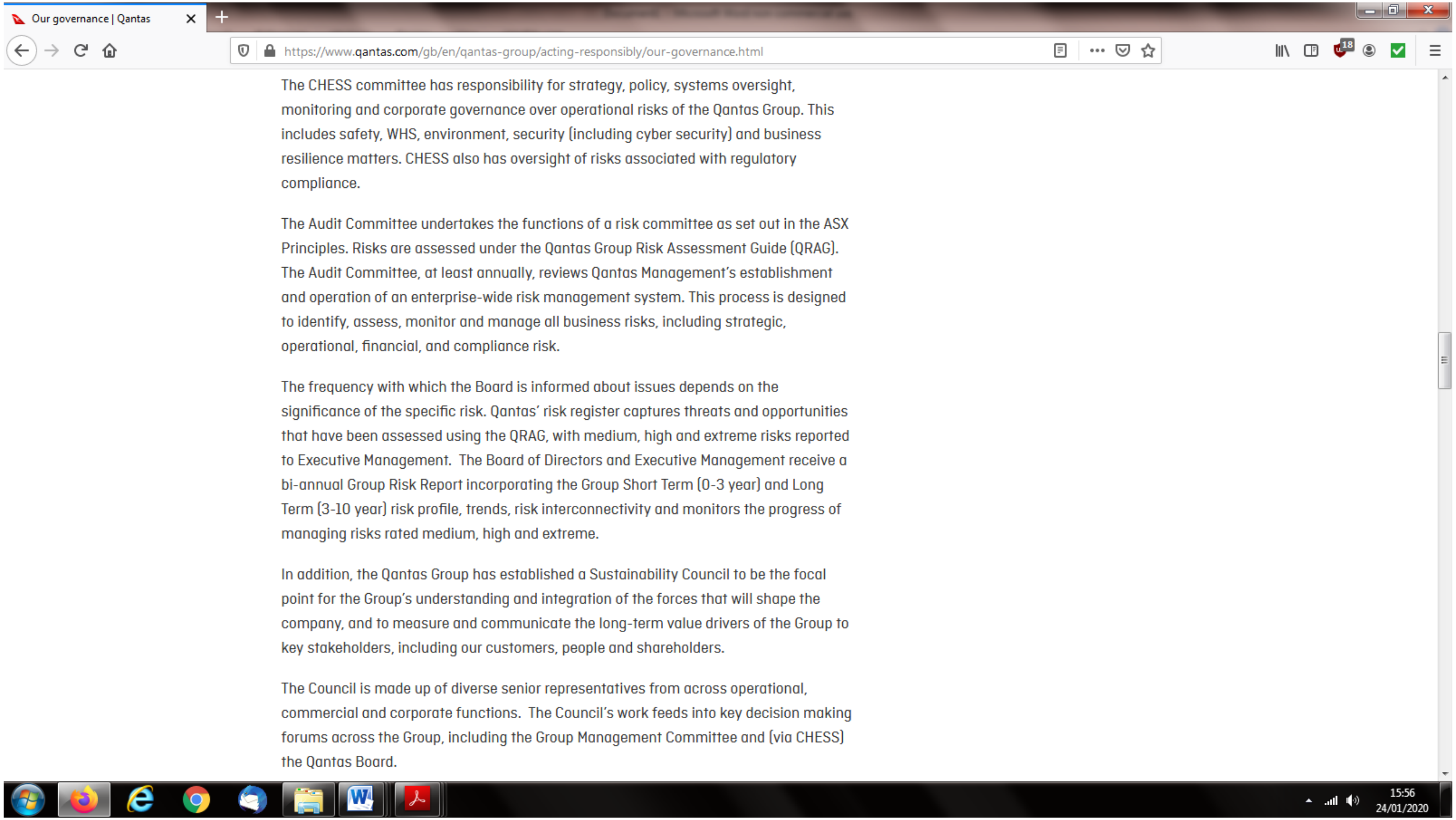
Operating in an industry with unpredictable internal and external risks is part of the Qantas Group's everyday operating environment, whether it's in the price we pay for fuel, business and consumer confidence levels, weather patterns across our global network, or broader geopolitical events. We are committed to managing the risks by strengthening business resilience and building an agile, adaptive culture - giving us the foundations for sustainable performance in all market conditions.

Our approach to risk management starts with our first priority: the safety of our customers and people. Qantas was one of the first airlines to introduce an integrated Safety Management System in the 1990s, and we continue to evolve it. Today we apply the same systematic approach to all risk disciplines, not just aviation safety. We integrate aviation operational safety, work health and safety, aviation and cyber security, environment (including climate change) and business resilience, learning from collaboration and shared experiences to make the system better.

Qantas maintains a strong governance structure for threats and opportunities. The Board has overall responsibility for the governance of risks. Oversight is maintained through the Audit Committee and the Committee for Health, Environment, Safety and Security (CHESS).

The CHESS committee has responsibility for strategy, policy, systems oversight, monitoring and corporate governance over operational risks of the Qantas Group. This includes safety, WHS, environment, security (including cyber security) and business resilience matters. CHESS also has oversight of risks associated with regulatory compliance.

The Audit Committee undertakes the functions of a risk committee as set out in the ASX Principles. Risks are assessed under the Qantas Group Risk Assessment Guide (QRAG).


Our governance | Qantas
https://www.qantas.com/gb/en/qantas-group/acting-responsibly/our-governance.html
15:56
24/01/2020

The CHESS committee has responsibility for strategy, policy, systems oversight, monitoring and corporate governance over operational risks of the Qantas Group. This includes safety, WHS, environment, security (including cyber security) and business resilience matters. CHESS also has oversight of risks associated with regulatory compliance.

The Audit Committee undertakes the functions of a risk committee as set out in the ASX Principles. Risks are assessed under the Qantas Group Risk Assessment Guide (QRAG). The Audit Committee, at least annually, reviews Qantas Management's establishment and operation of an enterprise-wide risk management system. This process is designed to identify, assess, monitor and manage all business risks, including strategic, operational, financial, and compliance risk.

The frequency with which the Board is informed about issues depends on the significance of the specific risk. Qantas' risk register captures threats and opportunities that have been assessed using the QRAG, with medium, high and extreme risks reported to Executive Management. The Board of Directors and Executive Management receive a bi-annual Group Risk Report incorporating the Group Short Term (0-3 year) and Long Term (3-10 year) risk profile, trends, risk interconnectivity and monitors the progress of managing risks rated medium, high and extreme.

In addition, the Qantas Group has established a Sustainability Council to be the focal point for the Group's understanding and integration of the forces that will shape the company, and to measure and communicate the long-term value drivers of the Group to key stakeholders, including our customers, people and shareholders.

The Council is made up of diverse senior representatives from across operational, commercial and corporate functions. The Council's work feeds into key decision making forums across the Group, including the Group Management Committee and (via CHESS) the Qantas Board.

4 / **1**.10 - Establish a BCMS conforming to the **Requirements** of *ISO **22301***

Cross Reference - ISO 22313 / **Context** - BCMS / 4.4

Note: This clause relates (in the main) ***only*** to an organisation intending to ***certify*** its BCMS to the ***requirements*** of ISO 22301. If this is not the case (e.g. you are instead ***aligning*** your BCMS with ISO 22301 / 22313 or 'doing something else / different') - then it (this clause) may be considered to be of an 'advisory' nature only - or might even be ignored

> The organisation shall establish, implement, maintain and continually improve a BCMS, including the processes needed and their interactions - and in accordance with the requirements of this document (latter refers to ISO 22301 / clause 4.4)

The above clause emphasises the need for the organisation to implement and maintain processes which will enable its BCMS to meet the requirements of ISO 22301:2019 - including all interactions between said processes

In determining the processes and their application throughout the organisation, it should:

- Determine the inputs required and the outputs expected from these processes
- Determine the sequence and interaction of these processes
- Determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes
- Determine the resources needed for these processes and ensure their availability
- Assign the responsibilities and authorities for these processes
- Address the risks and opportunities as determined in (ISO 22301) 6.1
- Evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results
- Improve the processes and the BCMS

To the extent necessary, the organisation should:

- Maintain documented information to support the operation of its processes
- Retain documented information so as to have confidence that the processes are being carried out as planned

Section **4 / 2** - **PLAN** - **RESOURCING** the **BCMS**

Cross Reference - ISO **22313** - 7.1 'SUPPORT / **Resources**'

Reminder: See 'important note' - page 18 - it also applies to ***all*** of this Section 4 / 2

As we have seen, the ***scope*** of BCMS related matters (in general) is related to the size, complexity, context etc. and the type of 'business' (what it 'does') itself of the organisation - and this applies equally to the acquiring / procuring etc. of all associated BCMS ***resources***

For smaller / simpler organisations resource requirements will typically be simply managed - with the opposite applying to e.g. large, complex, multi-national organisations - the latter including many airlines, airports, GHAs, MROs, Air Navigations Service Providers (ANSP) etc.

We now continue herein on the basis of the organisation being 'large and / or complex and / or extended / and / or multi-national etc.' - unless stated otherwise

A reminder here that we are still in the ***Plan*** phase of the PDCA cycle i.e. planning / preparing for how a BCMS will be introduced into an organisation. Consequently, this Section **4** / **2** should be used to ***provisionally*** identify and document the different ***types*** of ***resources*** which the organisation thinks it might (at this early point) need to support such planning & preparation

It should concurrently take the opportunity to start thinking of the ***additional***, longer term resource requirements to be put in place, to implement, operate, maintain etc. the BCMS. In ***later*** stages of this guideline document we will discuss in greater depth how these additional resource requirements are identified, approved / financed, established / procured, managed / allocated, reviewed, maintained etc.

The subject of 'resources' in general is of significant importance in operating an effective and efficient BCMS. All reference to same in ISO 22313 (for cross-reference info see page **105** of ***this*** guideline document) should be studied, understood and (where applicable) acted upon

At the outset of a BCMS introduction programme, it is **vital** to obtain the 'buy-in' and on-going support of the organisation's top management (TM). This extends to approval (in principle at this early stage) for the procurement / provision etc. of all appropriate resources + associated costs / budget etc. as related to **all** aspects of the BCMS (programme management) life-cycle

4 / **2**.1 BCMS **Resources** - General

ISO **22313** / SUPPORT / Resources - General and BCMS / 7.1.1 & 7.1.2

The organisation should determine the resources necessary to establish and implement (and, in due course, to operate, maintain, review etc.) the BCMS, throughout its ongoing life-cycle

The (eventual) availability of such resources, including during actual BC response operations, should be ensured by TM providing adequate oversight / review of the effective and efficient acquisition, storage, maintenance, replacement etc. of appropriate (resource related) requirements - intended to (in all and any ways required):

- Support achievement of BC policy, objectives, strategy, solutions, plans, ops etc.
- Be reliably available / 're-suppliable' within required timescales

- Be flexible enough to readily adapt to / facilitate change
- Facilitate associated communications e.g. with stakeholders / interested parties
- Facilitate ongoing maintenance, review and evaluation of the BCMS
- Facilitate the ongoing operation and continual improvement of the BCMS

Accordingly, adequate provision should be made for ‘resource’ related matters (as required) associated with the below considerations (*list is* ***not*** *exhaustive*):

- ***Identification*** (of required resources)

- ***Procurement*** (establishment of an ***appropriate*** ‘system’ if one does not already exist)

- ***Finance*** / ***Funding*** / ***Budget***

- ***People*** (in a ‘resources’ context):

    - Required commitment re the required time and effort involved etc.
    - Compensation arrangements? (e.g. ‘time-off in lieu; additional pay etc.)
    - Establishment of associated awareness, competence, testing / exercise etc.
    - A system for ‘managing’ people (HR) related issues re the BCMS etc.

- ***Facilities*** - e.g. work locations; storage of / ready access to resources; appropriate back-up / alternate facilities; supporting infrastructure etc.

- ***Equipment*** (including appropriate ICT hardware)

- ***Software & telecommunications*** (ICT)

- ***Fixtures & fittings***

- ***Utilities*** (including provision for backup measures e.g. UPS [uninterrupted power supply *system*], generators etc.)

- ***Maintenance and Resupply*** (of resources)

- A resources related ‘***controlled document’*** management system including e.g.

    - Policies
    - Requirements of Stakeholders and Other Interested Parties
    - Review
    - Legal etc. documentation (e.g. contracts, insurance policies, title deeds)
    - Terms of Reference
    - Other (e.g. budgets / finance; service level agreements [SLA])

- ***Communications in general*** etc. (typically with Stakeholders / Other Interested Parties)

4 / **2**.2 BCMS **Resources** - Identification (of)

Identification of in-scope BCMS related resources might typically be achieved via a series of ‘brainstorming’ sessions, conducted by those best suited for the task from within (and without if so required) the organisation

The organisation’s Business Continuity Manager (assuming that there is one - if not, this should be firstly addressed without delay [see also 4 / 2.5 - page 99]) should consult with TM on the matter. (Re TM - we are particularly [but not exclusively] referring here to the ‘BC Champion’ [assuming that there is one - if not, this should also be addressed without delay])

Such consultation should centre on who might best be able to provide the most useful inputs (during said brainstorming sessions)

In many organisations, employees from ‘middle level’ management (from all potentially involved departments / business units) are typically the most appropriate choices. If this is so and agreed, the line managers (of such middle level managers) should firstly be consulted as to which of the latter might be best suited for the task - with a view to making primary and secondary (back-up) nominations

The latter nominees are then briefed and interviewed (typically by the BC Manager) with the aim of confirming that they are indeed the most appropriate choices. Where the latter is not the case, the appropriate line manager should be requested to provide a more suitable candidate(s) and the process repeated. Where there is a shortfall (e.g. small organisation / low manpower base) the line manager might need to assume the responsibility directly

If what is written in the 2 paras just above is not acceptable to / possible for the organisation to comply with (for whatever reason) - suitable alternatives must be found by the BC Champion and BC Manager (e.g. in the smallest of organisations the latter two might be the most appropriate [and ***only***] choices for said brainstorming task; both roles might need to be combined etc.)

It might also be worth considering engagement of an appropriate (external) BCMS specialist consultant to assist e.g. either on an issue by issue basis or in a ‘more engaged / widespread’ capacity. The consultant ***must*** have an appropriate (***aviation*** related) background

Assuming that such nominations referred to above have been successfully made / approved, all involved should attend an ‘orientation’ course outlining the basics of BC / the BCMS and the absolute reliance of same upon resources (of all types - the basics of same being explained during the orientation training)

Following this, the brainstorming sessions are then conducted until the BC Champion and the BC Manager (or whoever) agree that all appropriate resource requirements have (probably) been identified. The results are then formally documented and presented to TM - with a view to approval and ‘permission to proceed’ i.e. budget for / obtain / procure etc. said resources

Most of what has been written above relates to ***resources*** required for the ‘**PLAN**’ phase of BCMS introduction. It should be repeated (as required) going forward - so as to ***similarly identify the resources required*** in the ‘**DO**’ phase - followed by the ‘**CHECK**’ and ‘**ACT**’ phases

4 / 2.3 BCMS **Resources** - Procurement

Further to 4 / 2.2 above, the organisation's 'Procurement' department / business unit is probably best tasked with obtaining what is required. If no such formal capability exists, an appropriate (organisation) person should be assigned - preferably with a deputy / alternate also nominated. Associated training / briefing / orientation should be provided as appropriate

It would obviously be beneficial (essential?) for all / any such person(s) mentioned just above to have been part of the brainstorming sessions mentioned in 4 / 2.2 (thus having also attended the associated orientation training)

Budget / finance will also be a significant consideration here, so this step 4 / 2.3 should run hand-in-hand with step 4 / 2.4 just below (also see again step 4 / 2.1 further above)

4 / 2.4 BCMS **Resources** - Finance / Budget

From the earliest phases of any BCMS project, the costs associated with acquisition, storage, maintenance, replacement etc. of associated resources should be estimated as accurately as possible, be approved by TM - and the associated budgets prepared, documented and issued

Note: It may be timely here for the organisation's BC expert (BC Manager or equivalent) to (diplomatically) remind TM that the introduction of BCMS is likely to lead to positive returns on any BC investment made. The latter can be both ***tangible*** (e.g. more customers / competitive edge; lower insurance premiums / wider insurance cover; reputation enhancement etc.) - and ***intangible*** (e.g. increasing stakeholder / interested party [e.g. shareholders, investors and employees] confidence)

Some typical resources for budget considerations include (NB: list is ***not*** exhaustive):

- ***Initial set-up costs*** - particularly the potential need to outsource BC 'expertise' (e.g. ***aviation*** related BC consultant[s]) for at least the introduction / implementation phase
- ***Cost of staff*** - salaries, allowances, incentives etc. e.g. employing a dedicated BC Manager; asking a current employee (typically Safety or Quality or Emergency Planning Manager etc.) to take on this 'extra' role - possibly at an increased salary?
- Costs re acquisition, equipping and maintaining a physical '***Disruption Response Management Centre***' facility + supporting infrastructure (see pages 100 -104)
- Costs related to acquisition, equipping and maintaining '***alternate***' location facilities e.g. for an **airline** these might include alternate locations for the ops control centre, for emergency and disruption management, for reservations & call centre, for critical ICT related systems etc. Similar considerations apply to **airports**, **GHAs** etc.
- ***Back-up power supply system****(s)* to critical facilities i.e. use of a UPS + Generators Again, within the airline / airport / GHA etc. context, critical facilities might typically include those requiring 'alternate location' consideration - as mentioned further above
- Matters related to ***Technology*** continuity i.e. ICT, data, backup resources etc. (latter often confusingly known [in the ICT context only] as 'Disaster Recovery')

- Matters related to ***Information*** (all forms / medias) & ***safeguarded storage*** of same
- Costs associated with initial & recurrent staff ***competency*** (training) and ***exercising***
- Costs associated with on-going ***monitoring***, ***reviewing***, ***maintaining*** and ***improving*** of the BCMS - including any external auditing costs (e.g. to maintain certification)
- etc.

4 / 2.5 BCMS Resources - People (ISO 22313 / 5.3 [particularly Table 3]; 7.1.2 and 8.4.4.1)

All personnel roles, responsibilities and authorities associated with BC should be defined and documented. All are subject to audit / compliance checks

People are the key to effective and efficient BC operations. A typical 'people' structure required to run a typical BCMS might look (top to bottom) something like:

- *'Top Management (TM)* ***BC Champion'*** - the organisation's TM should appoint a suitably experienced member of his / her executive team ('Top Management BC Champion' or similar title) to ***oversee*** (have overarching responsibility & accountability for) all aspects of the BCMS within the organisation

- *Higher Level Management* - '***BC Working / Steering Group***' - a specifically selected group of appropriately qualified / experienced etc. senior to middle level managers (reporting to the 'BC Champion') should be tasked with '***overall monitoring and executive troubleshooting***' of 'everything BC' within the organisation. Lower grade / rank staff with ***specialist*** knowledge might be co-opted to join this group - as required

  A prime responsibility for this latter team will be the mentoring, support, trouble-shooting intervention etc. of / for the organisation's primary 'specialist / expert' person(s) appointed to actually plan, implement, 'operate' and maintain (i.e. 'hands on') the BCMS on a daily basis......................i.e. the '***Business Continuity Manager***'

- The '***Business Continuity Manager***'

  Beyond doubt the best results for / from a BCMS will be obtained by using a dedicated, **FULL TIME** (sole responsibility) BC Manager. Ideally such person should already be reasonably familiar with **ALL** appropriate parts of the organisation (understanding the organisation) from the outset of the BC / BCMS introduction task. Thus an ideal candidate might be an experienced, relatively senior and longer term employee, * already working for the organisation in a role '***related***' to BC in some meaningful way e.g. an emergency planner, a risk manager, a quality manager etc.

  * As already mentioned the BC Manager should ideally ***not*** 'job-share' with other roles and responsibilities. However, it is recognised that in some organisations, this will not be possible

  Assuming that the requisite 'BC skills' (i.e. currently competent and tested [exercised]) are ***not*** yet in place, the next step would be to provide appropriate training for such person (typically sourced from an ***external*** BC training 'expert' - who **MUST** ***also*** be appropriately familiar with the type of business [i. e. ***aviation*** related {more specifically airline and / or airport and / or GHA etc. as required} for the purposes of this guideline document] conducted by the organisation)

An alternative option might be to hire an ***external candidate***, already qualified and experienced in BC matters + **having the appropriate, *aviation* related background**. The disadvantage here is that for large, complex organisations the 'understanding the organisation' requirement would take a considerably longer time to achieve (as compared to using an appropriate, internal candidate [if there is one])

To re-iterate, if hiring externally it is ***essential*** that such person be recruited from an essentially similar organisation e.g. from one major airline to another; from one large airport to another etc. so that he / she can 'hit the ground running', as best as possible

As at 2020, third party (external) Business Continuity expert consultants specialising in **aviation** related BC matters were **VERY** rare - consequently they will probably be quite expensive! Nevertheless, this option may need serious consideration, at least initially

- *The '**Workers**'* - When introducing a BCMS into an organisation there is an important requirement to not just gain buy-in and support from the management team - but also from the 'general workforce'. The (arguably not the clearest / most useful) BCMS term used to describe this requirement is '***embedding BC awareness** within the organisation*'. If achieved (typically not a quick and / or easy task) the resulting, general culture within the organisation should be overall 'pro BC'

  Of course, if staff at all levels (but especially at the middle to lower levels) clearly understand that BC can make a positive contribution to the 'bottom line' - they will also (hopefully) make the connection to their own security of employment and prospects. This will accordingly be an important concept to relay during the 'embedding of BC awareness' process

  However, and returning to people resources at the lower levels, a large organisation will typically require a relatively large number of such staff to respond to a major ***disruption*** event. Whilst a small number will ***manage, lead*** etc. - the great ***majority*** will actually carry out / provide the actual activities, processes, support etc. necessary to maintain / regain business continuity within the organisation (as related to the actual business area[s] adversely affected by any associated disruption event)

  For the purposes of ***this*** guideline document **only**, the title '**DISRUPTION SUPPORT UNIT** (**DSU**)' is used with regards to what is described in the para just above. The great majority of DSU staff will be ***directly representing*** the various departments / business units (to which they belong) within the organisation

  DSUs are typically formed & manned from / by the ***departments*** / ***business units*** reps directly associated with the particular type(s) of key main activities and / or key supporting activities etc. (together with associated processes / procedures etc.) which are ***predicted*** to require a BC response during a major disruption event

  DSU personnel require ***pre***-selection, training (initial and recurrent), exercising etc. - as an integral part of the organisation's ongoing BCMS management programme

For example, during a major ***airline*** disruption (e.g. closure of latter's major hub airport for a significant period) **DSUs** would ***typically*** be formed by reps from ***all*** / ***any*** of:

> Reminder - we are assuming a medium to large sized airline here. Smaller airlines will have significant problems providing manpower for the below DSU structure but, nevertheless, an appropriate 'workaround' solution ***must*** be found. **The below list is *not* exhaustive**. The titles used are 'generic. The same ***principle*** applies to ***airports***; ***GHAs*** etc.

- Aircraft Engineering / Maintenance
- Airline (Aviation) Planning
- Airport Services / Ground Operations (covering Hub[s] and Stations)
- Cabin Services (including cabin crew and in-flight catering)
- Cargo
- Commercial (including Reservations, Ecommerce and Marketing, Outlets etc.)
- Corporate Communications / PR (Internal, External & Crisis Comms)
- Customer Services (Call Centre[s] etc.)
- Facilities (including ground transport and accommodation services)
- Finance, Legal & Insurance
- Flight Operations
- HR
- Industry (Staff / Business) Travel
- ICT
- Operations Control Centre (disruption to flights, despatch, crewing etc.)
- Procurement & Logistics
- Safety ('Flight' and 'Ground')
- Security (both Aviation Security and General Security)

Individual **DSU** manning can range from just one person - to multi-person teams representing the larger departments / business units within an organisation

DSUs should be capable of operating 24 /7 / 365 if so required (e.g. to reflect associated airline / airport / GHA 24H ops). In such circumstances a **DSU** shift system is required (Reminder: manpower might be problematic here. However, associated 'workarounds' ***must*** be found)

Individual **DSUs** are typically ***led*** by middle to lower level managers and ***manned*** by lower level managers and (predominately) the general workforce

During a major disruption **all *involved* DSUs must** have representation at a suitable and central responding and management (command, control, co-ordination & communication - [C4]) facility - which might typically be termed (and as used herein) a '**Disruption Management Centre**' - **DMC** (see figure 7 - page 104)

During DMC activations - involved **DSUs** would typically send a rep to DMC meetings (anticipated as being ***several times daily***) whilst the remainder of the **DSU** staff (if any) perform assigned BC duties from ***normal work locations***. Where required by exceptional disruption circumstances, ***24H*** DMC operation & manning might be required

A back-up DMC (hot; warm; cold as required by the organisation's actual circumstances) should be planned for in case 'whatever causes the disruption' makes the primary DMC unavailable e.g. fire; unlawful act etc.

All **DSU** staff should be competent and experienced in their own, specific BC roles and responsibilities, via establishment of the appropriate competencies i.e. training (initial and recurrent), regular exercising and self-study of associated (their own) **DSU** BC response plans, procedures etc.

Documentation (appropriate reports, records, checklists, training manuals etc.) related to **DSU** activities & operations should be completed, maintained and retained - as required

IMPORTANT NOTE

This BCMS guideline document is just one of many produced by its author / owner (see ***separate*** document CRPM Part 3 / Volume 1 - page 49 for details). Most of the other guidelines relate to how airlines, airports and GHAs etc. plan for responding to a '***catastrophic aircraft accident***' type emergency / crisis i.e. ***nothing*** to do ***DIRECTLY*** with ***Business Continuity***. However, just as aviation BC ops need manpower resources, so do emergency / crisis response ops

Our manpower 'concept of operations' ***used for such emergency / crisis response ops*** is very similar to that described further above for **DSUs** - excepting the title (for airlines) would be '**Crisis Support Unit - CSU**' (instead of DSU)and the response (for airlines) is managed from a '**Crisis Management Centre - CMC**' (instead of a DMC)

CSUs typically need to use the same department / business unit <u>manpower</u> pools as DSUs

For ***<u>airlines</u>*** in particular, a ***worst case scenario*** for ***emergency / crisis*** response planning purposes might assume that the airline experiences (and needs to respond to) a catastrophic aircraft accident at its busiest airport - and that a knock-on effect of that accident is that this airport is closed for a considerable period e.g. a week or more - ***the latter causing concurrent, serious DISRUPTION to the airline's operations <u>AND</u> total shutdown of the associated airport***

The bigger the aircraft's seating capacity + the busier the airline - the bigger the problem. (Same principle applies [but in a different ways] to airports and GHAs)

In such realistic (worst case) scenario the accident ***airline*** would be deploying its **CSUs** and ***eventually*** its **DSUs** - managing both respectively from its (***<u>separate</u>*** facilities) **CMC** and the **DMC**. The 'worst case' scenario is also based (with good reason) on the airline also trying to conduct ***<u>concurrent</u>*** '**normal**' operations across its network - ***other than at the accident airport itself***

What all of the above means in reality is that (when considering manpower resources for worst case ***emergency / crisis*** type scenarios as described above) - ***airlines*** must ***also*** plan to provide (ideally separate) manpower resources for ***eventual BC ops*** - ***AND*** to also account for *ongoing* ***'normal' business*** *ops.* This will obviously cause major manpower resource problems for any airline. Nevertheless, this might be the actual situation 'on the ground, on the day' - and must thus be ***managed*** (and ***pre-planned*** for) and appropriate solutions found (even if they are ad-hoc / workaround / temporary in nature)

Using the same worst case scenario (i.e. total airport shutdown) - it might seem that the accident ***airport*** is relatively 'better off' than the accident airline - as it (the airport) needs to conduct just (only) emergency / crisis response ops until such time as it re-opens for business (on the basis that whilst it is closed there is no business - consequently there cannot be a business continuity problem!!!)

Whilst preparations for ***airport*** re-opening will obviously be necessary (e.g. removing accident aircraft; recovering and removing human remains and personal effects; repairing damage to airport infrastructure etc.) - these do not pedantically relate to 'business continuity' type ops

However, it is highly likely that the accident airport (assuming here that it is large and busy) will have thousands of persons ***already there*** at the time of the accident. Some will be arriving and departing passengers and some will be family, relatives and friends etc. (meeters & greeters) of said passengers. Others will be airport staff and employees e.g. of the various commercial outlets (shops, restaurants etc.) found at the airport

A significant 'complicating' factor is that some of the above persons will already be 'airside' at the airport - and some 'landside'. Equally significant is the likely probability that very large numbers of 'local' persons (not having been at the airport at the time of the accident) also eventually come to the airport, for various reasons not expanded upon here. Lastly, a very high proportion of all such persons mentioned above will be exhibiting various degrees of anxiety, distress, anger etc.

So, ***in reality*** the accident airport in this scenario ***does*** have a **BIG** problem and, whilst (arguably) not a business continuity matter, the problem must both be managed and be seen (by the world if necessary) to be being managed. It is in these last two areas that the airport's business continuity capabilities (assuming it has them) would be targeted - regardless of the pedantics, titles, terminology etc.

In contrast - and for ***airports*** which might have the capability of responding to a catastrophic aircraft accident 'on-airport' ***and concurrently keep the airport open for operations*** (e.g. parallel runway ops might permit same provided approval from the appropriate authorities [Civil Aviation Authority; Air Accident Investigation Agency etc.] was forthcoming) - then such ***airports*** would need to ***pre-plan*** for a similar situation as described further above for ***airlines*** i.e. operating the ***airport's*** emergency plan **+** ***business continuity plan*** concurrently - whilst **also** trying to maintain '***normal***' ops. The same, extreme demands on manpower resources (i.e. similar to the airline situation described above) would apply

Ground Handling Operators ***may be the hardest hit of all*** (regarding manpower resources) as they may be considered to have emergency response, business continuity and normal operations accountabilities to both client ***aircraft*** operators and to their parent ***airport***. They (GHAs) would ***also*** need to ***concurrently*** respond to their ***own*** continuity aspects of the disruption and normal ops demands - as appropriate to actual circumstances 'on the day'

Lastly, whilst this 'important note' relates (for simplicity) to ***manpower*** resources, ***other types of resources*** would be similarly impacted by the need to provide ***two*** contingency response operations concurrently (emergency / crisis response ops + BC ops) whilst ***also*** maintaining concurrent ***normal*** ops. For example, it would typically (but not necessarily always) border on recklessness to pre-plan on concurrently responding to the emergency / crisis and the knock-on BC situation, whilst operating from the same command & control facility i.e. **SEPARATE** **CMC** and **DMC** facilities **MUST** typically be pre-planned for, resourced accordingly (including manning) and operated - as required 'on the day'

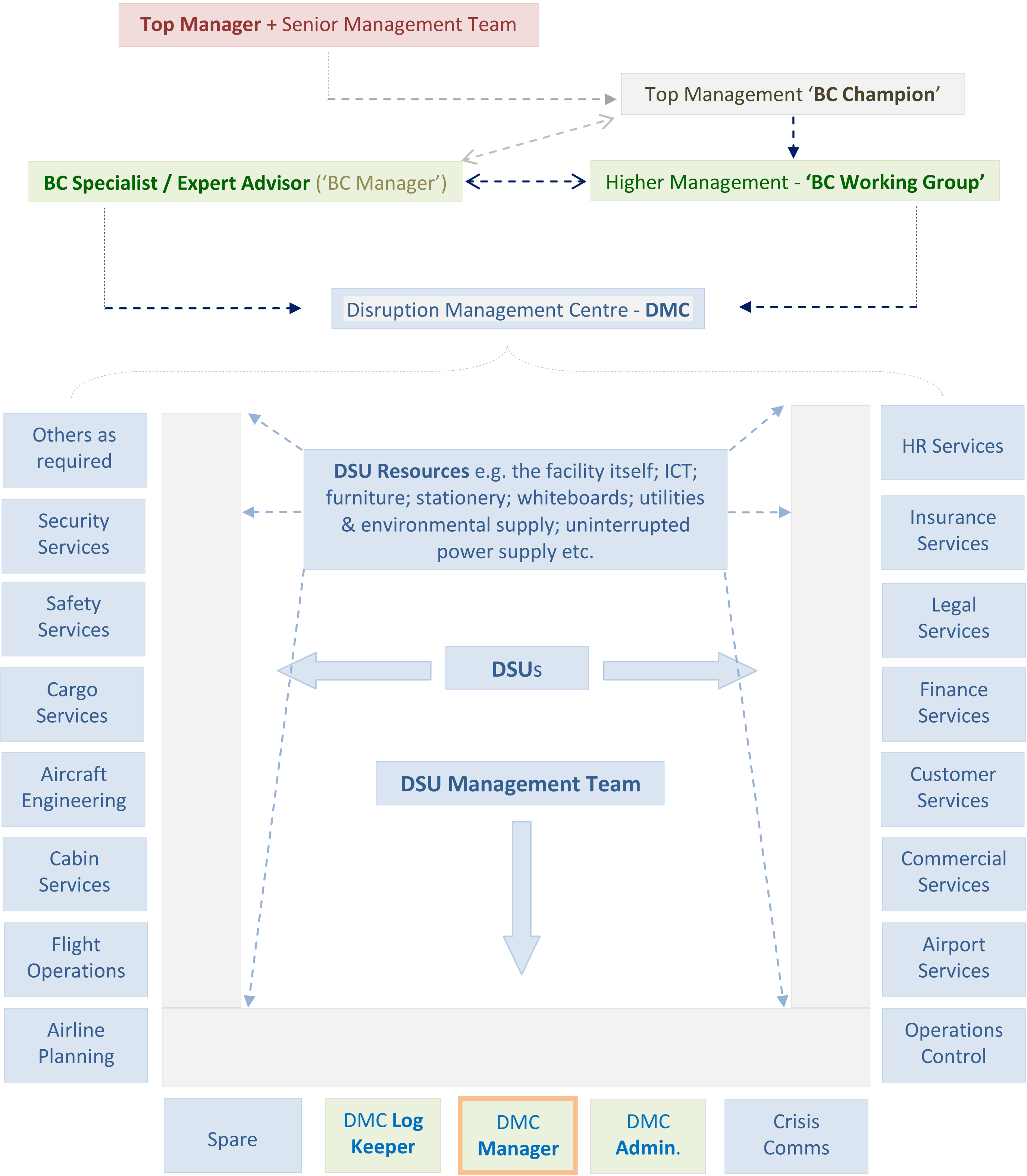


Figure **7** - A typical **Airline DSU** Layout (airline departments / business units shown are for representative purposes only)

4 / 2.6 - BCMS Resources - **Infrastructure; Facilities; Equipment**

Technology; Information etc. (ISO 22313 / 7.1.2)

The above resources and similar have already been referred to in the General (4 / 2.1) and Finance / Budget (4 / 2.4) sections further above

4 / 2.7 - BCMS Resources - **Documentation**

(ISO 22313 / 7.1.2)

The 'BC Resources Programme' should be appropriately documented. See *Sub-section **4 / 6*** (page 113) of ***this*** guideline document (the one you are reading now) for more information

For cross reference purposes, the subject of *BC **resources*** also appears herein at:

Section 4 / 1 / 3 of this guideline (page 67) - based on:

ISO 22313 / 5.1 to 5.3 - **LEADERSHIP & COMMITMENT**

Section 4 / 2 of this guideline (page 95) - based on:

ISO 22313 / 7.1 - '**SUPPORT** / Resources'

Section 5 / 2 of this guideline (pages 135 & 192) - based on:

ISO 22313 / 8.2.2 - **OPERATIONS** / BIA

Section 5 / 3.5 of this guideline (page 215) - based on:

ISO 22313 / 8.3.4 - **OPS** / BC Strategy & Solutions - Resource Requirements

Note 1: The subject of 'resources' gets a significant number of ***additional*** 'mentions' throughout the whole of (ISO 22313) - ***Clause 8***. These 'mentions' should all be noted and, where appropriate (e.g. if it is an organisation's intention to ***certify*** to the requirements of ISO 22301) acted upon as required. Access to the (latest versions) ISO 22301 and 22313 standards would be necessary for this to be accomplished. However, what is referred herein (i.e. in the document now being read) - on the subject of 'resources' - should be sufficient for those organisations wishing to ***align*** (i.e. ***not*** 'certify') with ISOs 22301 / 22313

Note 2: - there is significant overlap in the resources related info provided in ISO 22313. Little effort seems to have been made (by the ISO Technical Committee which produced it) to better manage / mitigate same (which may thus be potential sources of confusion to some users / readers)

Section **4 / 3** - **PLAN** - EMBEDDING ***AWARENESS***

Cross Reference - ISO 22313 - 7.3 ‘**SUPPORT** / Awareness’

Reminder: See ‘important note’ - page 18 - it applies to ***all*** of this Section 4 / 3

The term ‘embedding awareness’ is a ‘not so simple’ way of saying that just about everyone relevant / appropriate in an organisation, top to bottom, should be:

- Reasonably aware of the organisation’s BCMS related matters, in general

- Personally aware of specifically assigned BCMS roles, responsibilities, accountabilities etc. (if so assigned) - together with their associated contexts i.e. where do they (and the person[s] ‘doing’ them) ‘fit in’ with others similarly involved?

The organisation should ensure that the above concept of ‘BCMS awareness’ extends (insofar as is necessary / possible / desirable etc.) to any other stakeholders / interested parties (where appropriate / to the extent possible) e.g. external suppliers, contractors, appropriate ‘authorities’ etc.

All concerned should be aware (to the appropriate degree) of the organisation’s associated BC Policy, Objectives etc. - together with associated roles, responsibilities, accountabilities etc. related (as applicable) to :

- Achieving conformity with the organisation’s BCMS requirements
- Reducing the likelihood and impact of disruption before it might occur
- The concept of ‘safety first’ i.e. self-protection, evacuation etc.
- Disruption detection + response / mitigation + continuity / recovery of ops etc.
- Dependencies on suppliers and similarly outsourced services etc.
- Implications of change (within and / or without the organisation)
- Individual and team contributions to the effectiveness of the BCMS
- The BCMS becoming part of the organisation’s core values, management activities etc.
- Instilling increasing awareness, accountabilities etc. amongst stakeholders / interested parties - particularly those from outside the organisation
- The associated (potential) benefits of BC to all concerned

Such awareness should lead, in turn to e.g. (list is not exhaustive):

- More effective, efficient, expedient etc. development, operation, maintenance etc. of the BCMS = better mitigation re the likelihood and adverse impacts of disruption
- Increasing confidence in the organisation’s ability to handle disruption
- Increased resilience e.g. by ensuring BC type considerations are considered and accounted for (as required) at all appropriate levels of organisational decision making

The concept of ‘embedding BC awareness in an organisation’ is good in principle - but can be difficult to achieve in reality. Some reasons for the latter include:

- Some personnel, already overworked with regard to their ***primary*** (non-BC related) duties, might be ‘asked’ to take on additional BC related accountabilities / responsibilities (typically [but not always] without associated reward / compensation)

  This is typically due to them being the only people (in the organisation) capable of ‘achieving what is required’ in certain areas of the BC context (e.g. an organisation’s safety manager / emergency planning manager [single person - already having ***dual*** accountabilities] - now being assigned ***additional*** BC accountabilities)

- BC responsibilities typically only ‘drill down’ as far as those involved at **DSU** level, leaving many staff outside of the ‘BC awareness loop’ - no matter how much the subject is ‘advertised / promoted’ within the organisation. For example, BC awareness programmes, no matter how ‘well managed, resourced etc.’, will be of little or no interest to some staff - and thus will be ignored, if possible so to do

- Staff turnover i.e. BC trained and / or aware staff leave the organisation and are possibly replaced with staff who fall through the BC awareness net e.g. through not including BC in new staff induction training / further awareness programmes

- A fairly natural human reluctance to embrace change - whatever the potential benefits

- For most personnel within an organisation the benefits of BC are ‘intangible’

- An unwillingness to assist the organisation outside of contractual, employment terms

- A ‘blame culture’ within the organisation - making staff fearful of getting involved with anything (where blame might be attributable) over and above their basic duties

On the plus side, we have already seen some of the benefits of running a BCMS programme within an organisation (see page 41) - a number of which might be directly advantageous to all staff i.e. better rewards (e.g. increased profits might = increased staff profit sharing and / or pay increases); security of employment; ability to diversify; better job satisfaction etc.

So what will probably be a long & possibly difficult process of ‘embedding BC awareness’ - may be well worth persevering with and, if implemented sensitively, logically and fairly - could well enhance (even if only in the longer term) the experience of working within the organisation

We have also already mentioned herein the concept of ‘***understanding the organisation***’ (see page 53). Such understanding makes a vital contribution in working out the best way to embed BC awareness

BCMS awareness can be achieved directly (e.g. via training & exercising etc.) by those having formal BC roles & responsibilities. Additionally, various other methods may be employed to raise awareness amongst ***all staff*** (having BC roles / responsibilities or not) including:

- Fostering commitment to organisation’s Mission Statement, BC Policy / Objectives etc.
- Briefings for Top Management
- Workshops

- Information documentation (newsletters, flyers, short info brochures etc.)
- Regular awareness programme via the organisation's internal communications setup (e.g. via email; via websites / intranet; via simple eLearning systems etc.)
- Incorporation within induction programmes for new staff
- Inclusion of BC as an ongoing topic during department / business unit / team meetings
- Publication of 'post BC incident' feedback / reports / corrective action taken etc.
- Visits to alternate hot / warm / cold BC recovery sites / locations
- BC participation linked to pay and promotion prospects where possible / feasible
- Establishing and publicising 'rewards and / or recognition' opportunities for involvement with BC
- Competitions, quizzes etc. - with desirable rewards (for an airline the rewards might be low cost but highly desired by 'contestants / participants' e.g. space available first / business class flights + accommodation [to winner and spouse] to any destination on the airline's network; access to airport first / business class lounges; shopping vouchers etc.)
- Use of internal publicity related to BC *exercise* planning and feedback + the actual exercises themselves - to reach out to as wide an audience as possible - even those not directly involved with such exercises

High profile BCMS awareness campaigns should be run before and during the ***initial*** introduction and implementation phases of the BCMS - with the intent that 'everyone' understands the associated reasons and benefits. Following this, similar campaigns might be run from time to time - once the actual BCMS plans and supporting infrastructure etc. are in-place / operational

It is important to win over ***middle management*** staff, as many are very experienced and typically understand the organisation very well (at least in parts). Accordingly, they will almost certainly be drawn in (in one way or another) to BCMS activities, voluntarily or otherwise. '***Voluntarily***' is obviously preferred - and extra care should be taken in efforts to get them 'pro-BC' - rather than trying to impose it (the latter will typically not work - at least not to the degree necessary to achieve the desired outcomes, as painlessly as possible!)

It is also particularly important to win over those involved with ***procurement and logistics*** i.e. those dealing with external suppliers, outsourcers, intermediaries etc. If the former are pro-BC, it is more than likely that they will, in turn, try to ensure similar is engendered in the latter

Furthermore, BCMS awareness can be increased by communicating same to those outside of the organisation i.e. to external stakeholders / other interested parties whoever they might be - from suppliers to regulators; from customers to shareholders. The potential benefits of doing this can be significant (again, see page 41)

Lastly, awareness re external changes to BC / BCMS in general (e.g. updates to associated ISO standards / associated material; BCMS related global 'trends' etc.) can be achieved by e.g. the organisation actively participating in local / national / international BC type activities such as associated interest groups; conferences; being a member of a BCMS associated ISO Technical Committee etc. (e.g. ISO TC 292 [Security & Resilience] produces ISOs 22301 and 22313)

Section **4 / 4** - PLAN - ACHIEVING ***COMPETENCE***

Cross Reference - ISO 22313 - 7.2 'SUPPORT / **Competence**'

Reminder: See 'important note' - page 18 - it applies to ***all*** of this Section 4 / 4

The organisation should establish an appropriate and effective system for establishing, maintaining, reviewing etc. all competence related matters relating to persons (under its [the organisation's] control and / or on its behalf) undertaking associated BCMS work, duties etc.

All (of an organisation's) BC designated responders, at **all** levels, **must** acquire and maintain a reasonable (pre-defined by the organisation) level of ***competence*** in whatever it is that they will undertake during actual BC ops i.e. as related to the general concept of the organisation's overall BCMS and their place in it; specified roles / responsibilities etc. This is typically achieved via a formal regime of (associated) initial and recurrent training, exercising and further development (as required for latter - see next para below) (ISO refers to the above as a 'competence development programme')

Staff specifically responsible for the ***management*** of actual BC 'command, control, co-ordination and communications' (C4) ops **must** additionally acquire and maintain the knowledge level status of '***expert***' in **all** aspects of the organisation's BCMS - theoretical and practical (the word / concept of 'expert' not defined herein - but should be interpreted in its logical / common use context)

It is highly desirable that a BC '***train the trainer***' programme is initiated, drilling down to **DSU** level, so that they (DSUs) eventually develop capability in conducting their ***own*** (in-department / business unit) BC training and modular exercises (typically under the [continuing and overarching] oversight of the BC Manager - to whom they should always remain accountable)

Depending on the organisation, general awareness (and competence etc.) resources can come from within the organisation itself e.g. via the BC Manager conducting the training and exercising programme; via the DSUs; via eLearning etc.

Said resources can also be outsourced ('instead of' and / or 'additional to' internal training). A major disadvantage of same is that there will typically be a lack of appropriate '***understanding the organisation'*** (by said outsourced trainers) compared to the in-house option. Furthermore, there are very, very few external BC experts (trainers) in the world capable of adequately delivering such training in an AVIATION related context

Note: It might also be necessary to pre-establish 'competence' (if not already so competent) for those tasked with introducing the BCMS into the organisation in the first place i.e. in contrast with the conduct of actual BC ops). For more on this see appropriate text of section 4 / 1.3 (starts page 66)

Note - BC training is a statutory (legal) requirement within some organisations e.g. in ***UK*** all 'blue light' emergency services (police, fire & ambulance); local authorities (city, county, town etc.); regional health authorities etc. are legally required to have BC plans in place and to conduct associated training and exercising. This was mandated by the UK's 'Civil Contingencies Act (Law) - 2004'. The above also applies to UK ***airports*** **BUT**, paradoxically, not to UK ***airlines***!

As an example, the following 'competence development programme' might be planned for, resourced, implemented, maintained, evaluated / reviewed…………………:

- Identify, define & document required BC competencies and those that they apply to
- Identify and document training requirements - as associated with BC competencies
- Produce / procure the associated training / study notes; cross-references etc.
- Procure / establish any other required training support resources
- Identify, engage and establish / prepare the trainers (external; train the trainer etc.)
- Decide ***who*** (which target groups; individuals etc.) receives ***what*** training (e.g. 'initial', 'advanced [expert]', 'recurrent', 'train the trainer' etc.) - ***when*** (e.g. six monthly; annually) - to ***what levels*** of competence (e.g. basic, intermediate, advanced, expert etc.) - and ***how*** (e.g. classroom; self-study; CBT / E-learning; practical etc.)
- Deliver appropriate types of training to target groups – as per bullet point just above
- Monitor & measure training delivered versus attainment & retention of same
- Maintain the competence development programme
- Periodically evaluate / review the competence development programme
- Strive to continually improve the competence development programme
- Establish, maintain and improve BC skills / experience - by establishing a regular and specifically targeted BC '***exercise***' regime / programme
- Ensure thorough and timely feedback follows each such exercise
- Ensure that such feedback is adequately 'analysed' so that appropriate corrective and similar action might be taken - as required
- Consider 'cross-training' of appropriate staff re their normal business duties so as to provide potential flexibility during any actual BC operational response
- Control and maintain all associated documentation (reports and records etc.)

Personnel from external parties (engaged by the organisation on ***longer term*** projects) should be contractually required to attain, retain and demonstrate an appropriate level of BC competence (as appropriate) - as related to the work for which they have been engaged

The organisation should make every effort to ensure (insofar as is permitted / practicable) that external parties involved in e.g. the organisation's 'supply chain' (re e.g. 'supplies' categorised as 'critical' to the continuity of the organisation's product / services / operations) also achieve / maintain an associated and appropriate level of BC competence

The expedience / quality of BC competence achievement & retention might be considerably enhanced if the organisation makes same a formal part of its HR rewards / recognition / performance / appraisal process

The latter two (performance & appraisal) , require, in turn the issue of formal BC terms of reference and / or BC role / job / task / skills set descriptions - against which performance can be monitored / measured / evaluated / improved - which is exactly what is required

Active participation by top / senior management in BCMS related training and exercising etc. obviously sets a 'good example' and should be actively encouraged / lobbied for (as required)

Section 4 / 5 - PLAN - COMMUNICATIONS

Cross Reference - ISO 22313 - 7.4 'SUPPORT / **Communication**'

For related matters - see also ISO 22313 - 8.4.3 and 8.4.4.5

See also the '**DO**' Section of this guideline - 5 / 3.8 (page 219) - for additional guidance

Reminder: See 'important note' - page 18 - it applies to ***all*** of this Section 4 / 5

Communication (with Stakeholders / other Interested Parties)

Effective, efficient, co-ordinated, consistent, comprehensive (where needed), accurate, timely, flexible, honest / transparent etc. ***communications*** are an essential component of any contingency response, including business continuity operations

All available and appropriate methods of conducting communications should be considered.

The following should be addressed - as required:

- The BC 'communications' expectations of 'stakeholders / other interested parties' (* internal & external to the organisation) should be identified and adequately accounted / planned for. In certain circumstances, 'who' is to be communicated with, how, when, why and 'related to what' might be mandated (e.g. legal / regulatory requirements etc.) e.g. with regards to emergency services and similar

  * Internal (within the organisation) communications are particularly important during contingency operations e.g. those related to emergency / crisis response; BC operations etc.

- Further to the above (and as appropriate) the organisation should use pre-researched / defined threshold guides beyond which it might typically be necessary to 'start communicating' - in some meaningful way, shape or form - with whoever might be the subject (s) of the communications

- The frequency of such communications will probably relate to 'what the organisation does' (i.e. the organisations key activity / activities, operation(s), product(s) etc.) - combined with the associated (typically adverse) impact(s) related to any particular disruption event

- For smaller / simpler organisations - 'who needs to be communicated with' should be relatively easy to work out. For everyone else it will be like asking the question - 'how long is a piece of string'? The simplest answer is that most (if not all) known stakeholders / other interested parties will be considerations. However, during the aftermath of a major disruption event it is highly likely that 'previously unknown' stakeholders etc. will become apparent - and should thus also be communication considerations. Bottom line might be to deploy flexible comms priorities in accordance with actual circumstances in play 'on the day'

- All methods / mediums of BC comms (available and appropriate to the organisation) should be considered e.g. written (hard & soft copy); spoken (training, briefings etc.); the world wide web, social media, the press, TV and radio, press conferences etc. Primary method(s) of communication chosen should have at least one backup / alternative method 'ready to go'. The organisation may include references to its BCMS and associated matters in supplier, customer and similar (external) newsletters, briefings etc.

- ***Back-up*** (*alternative*) means of conducting BC related communications should be procured / established and regularly maintained / tested. This particularly relates to ICT type / related data backups. Associated competence is required

- The communication needs of the organisation's 'BC alerting & activation system' should be accounted for - particularly those which are ICT related / operated etc. Associated competence is required

- Appropriate staff (e.g. Top Manager & deputy; DMC Managers; the *Corporate Communications / PR* Disruption Support Unit [DSU]) Manager etc.) should achieve / retain an appropriate level of competence / experience in BC crisis communications - including acting as 'spokespersons' for the organisation i.e. being its 'public face' at time of crisis etc.

- A capability should exist to adequately adapt / integrate / activate external alerts (e.g. national / regional / local threat advisory systems & similar) into the organisation's communication system, where and if appropriate

- Establish an 'operation and testing' (exercising) regime re the organisation's BC communications capabilities

- Appropriate resources should be provided for (including budget / finance) - re adequate and timely procurement / implementation / maintenance etc. of all of the above, together with associated dependencies, together with an adequate contingency allowance etc.

- The organisation should provide / employ effective communications as part of its awareness programmes and throughout actual BC type operations

- A documented system should be established to manage and record appropriate matters associated with all of the above. The system should include a comprehensive, current and accurate database of contact information necessary for the organisation to alert, activate, manage and operate an adequate BC response

Section **4 / 6** - PLAN - **DOCUMENTED INFORMATION**

Cross Reference - ISO 22313 - 7.5 'SUPPORT / **Documented Information**'

Reminder: See 'important note' - page 18 - it applies to ***all*** of this Section 4 / 6

Purpose of Establishing, Maintaining and Retaining BCMS Related Documented Information?

To provide ***documented evidence*** of the effective preparation, implementation, operation, maintenance, monitoring, measuring, reviewing and continual improvement of an organisation's BCMS i.e. evidencing conformity to appropriate BCMS requirements, guidance, recommendations; the effectiveness of associated operations etc.

(Quote) .... 'To the extent necessary the organisation should maintain & retain documented info to support operation of BCMS processes and have confidence that the latter are being carried out as planned' (ISO 22313 - clause 4.4)

General

If an organisation intends to prepare and **formally certify** its BCMS to the **requirements** of ISO 22301 (as guided / recommended by ISO 22313) - all of the required documented information **must** be established, maintained, retained etc. Additional, documented information ***may*** also be required e.g. to ensure the effectiveness of the BCMS (See next page for further details)

If an organisation intends instead to prepare and **formally align** its BCMS with the **guidance** & **recommendations** of ISOs 22313 - then following the same 'documented information' requirements (as per the last para above) is recommended

If an organisation wishes to use ISO 22313 to ***informally guide*** its BCMS preparations in general, the guidance / recommendations (as per above) might still be followed, insofar as is deemed compatible with the size, complexity, context, nature of business, risk appetite etc. of the organisation concerned and / or associated decisions made by its top management

Note: For organisations intending to ***certify*** or ***formally align*** their BCMS with ISOs 22301 / 22313 respectively - the latter's clause 7.5 (Documented Information) should be 100% complied with

Documented Information - Creating / Updating; Access to; Types of Control

The vast majority of airlines, airports, ground handling agents etc. will already be familiar with the requirements / operation of a '***controlled document system***' - as an integral part of 'what they do' during normal ops. Accordingly, those aspects of 'documented information' contained in the above title have been * ***excluded*** from this guideline's scope (**IMPORTANT**: ***without*** such a ***system*** in place, the task of planning, implementing, managing etc. a BCMS will possibly be considerably more ineffective, inefficient, confusing etc. than it otherwise might be)

* Readers / users etc. requiring further details re the above should gain access to ISO 22313:2020 (however this might be achieved - see page 45 for suggestions) - and refer to clauses 7.5.2 and 7.5.3

Confidential, Personal, Proprietary & Similarly 'Protected' Documentation

Appropriate care should be taken to ensure the appropriate protection / safeguarding / non-disclosure etc. - of confidential, personal and similarly 'sensitive' documented information

Furthermore, full compliance should be established with all relevant / applicable legislation, regulation, code etc. (including appropriate 'data protection / personal privacy' and similar issues) regarding the acquisition, use, transfer, retention etc. of documented information. Associated processes etc. should be established and maintained - with regards to same

Documented information includes (ISO 22313 clause cross-references in brackets) includes:

- Understanding the organisation and its context (4.1)
- Legal and regulatory requirements (4.2.2)
- BCMS Scope - including any exclusion(s) (4.3)
- BCMS Policy (5.2)
- BCMS Objectives and planning to achieve them (6.2)
- Competence (7.2)
- 'Stakeholder', 'Business Impact', 'Risk Assessment' & 'Resources' Analyses (Part 8.2)
- Business continuity strategies & solutions (including options considered for latter) (8.3)
- Business continuity plans and procedures (8.4)
- Exercise programme (8.5)
- Monitoring, measurement, analysis and evaluation (9.1)
- Internal audit (9.2)
- Management review (9.3)
- Nonconformity and corrective action (10.1)

Some examples of additional BCMS related documented info for consideration (In no particular order. The list is not exhaustive)

- Contracts, service level agreements etc. (typically those with BC implications)
- Awareness programmes
- Training (competence) and exercise programmes
- Communications with stakeholders / other interested parties
- Results of 'Stakeholder', 'Business Impact', 'Risk Assessment' & 'Resources' Analyses
- Exploring and selecting most appropriate BC tactical solutions / treatments / controls
- Emergency / Crisis (Incident) response plan overviews (i.e. ***not*** BC *plan* overviews)
- Risk (and thus BC) monitoring of (external service, product, operation etc.) providers
- Evidence and results of inspection, maintenance, measuring, calibration etc.
- Post-incident reports of incidents and near-incidents
- BCMS review meeting minutes etc.

Note to User / Reader

We are now leaving the **‘PLAN’** section of this guideline document and moving on to the **‘DO’** section i.e. we have finished pre-planning / pre-preparing - and are now ready to start ***‘doing’***
(i.e. the ‘implementing & operating’ part of the PDCA cycle)

Section **5** - DO - **DEVELOPING the BCMS**

Supplementary Contents List for this Section 5 ***Only***

Reminder: See 'important note' - page 18 - it applies to ***all*** of this Section 5

Section 5 / 1 - DO - DEVELOPING the BCMS / Operational Planning & Control

Cross Reference - ISO 22313 - 8.1 / OPERATION / '**Operational Planning & Control**'

In this '**DO**' phase of the PDCA cycle the organisation is required to ***implement***, ***control, operate*** etc. its BCMS needs and requirements (via associated processes etc.) as already determined in Section 4 of this guideline document i.e. the various ***elements*** of the required business continuity ***programme management*** project must now be ***actually established*** (put in place) and ***effectively documented / managed*** / ***maintained / reviewed*** (as required) etc.

The 'control' referred to above typically includes / applies to (list is ***not*** exhaustive):

- Invocation (establishing) of the ***implementation plan*** and associated ***methodology*** - as should have ***already*** been ***pre-prepared*** as per Section 4 of this guideline document
- Integration of the above with organisation's normal business processes where possible
- Measurement of ***project progress*** e.g. by specifying specific deliverables; by use of project milestones etc. (Reminder - the usual project management 'tools' [GANTT & PERT charts etc.] can be used here if required)
- Ensuring outsourced considerations (processes; supply chain etc.) are controlled
- Operating an appropriate 'change management' system
- Maintaining an associated 'documentation management and information' system

Elements of Business Continuity Programme Management (BCPM) - (ISO 22313 - 8.1.2)

See again Figure 2, page 47 and figure 3, page 49 - as required

The major elements of Business Continuity Programme Management (***BCPM***) comprise:

- ***Operational planning & control*** (you are reading about this ***now*** [ISO 22313 - 8.1])
- ***BIA , RA*** etc. (otherwise known as 'understanding the organisation' - and covered later in Sub-section 5.2 of ***this*** guideline document [cross-reference ISO 22313 - 8.2])
- Deciding the appropriate ***BC strategies*** to use and then further deciding how they are to be achieved (primarily [in the BC context only] by selection & use of associated & appropriate 'BC ***Tactical Solutions*** / Treatments / Controls' - all of ***this*** also being covered later in Sub-section 5.3 of ***this*** guideline document [cross-reference ISO 22313 - 8.3])
- '***Make it all happen***!' (& then maintain & evaluate it) e.g. produce the associated BC & business recovery plans / procedures; set-up an appropriate 'BC (disruption) response structure' - including acquisition of associated resources (particularly manpower); establish required degrees of competency (training) & experience (exercising + actual BC operations [if any for latter]); maintain and evaluate the BCMS etc. - all covered later in Section 5.4 of ***this*** guideline document (cross-reference ISO 22313 - 8.4 & 8.5)

The initial establishment and ongoing management tasks etc. of BCPM should be assigned to the designated personnel resources (which should have already been identified, documented, trained and appropriately resourced etc. - as per Section 4 of this guideline document)

Maintaining Business Continuity (and thus BCPM and the BCMS) - (ISO 22313 - 8.1.3)

Effective maintenance of 'BC' includes:

- Ensuring ongoing relevance of associated BC scope, roles & responsibilities etc.
- Embedding / promoting BC within the organisation and 'anywhere else' (required / permitted)
- Managing associated costs and other financial matters
- Establishing / monitoring an associated change / succession management process
- Providing for appropriate and ongoing training and awareness etc.
- Providing for appropriate and ongoing exercising / testing etc.
- Maintaining / retaining / safeguarding of associated (appropriate) documentation
- Appropriate and ongoing review and update (as required) re all of the above (particularly if e.g. significant change impacts on the organisation's operational environment, structure, locations, personnel, processes, technology etc; e.g. when an exercise or actual incident highlights deficiencies - and so on)

Measures aimed at ensuring that BC remains as effective and efficient as possible, include (list is ***not*** exhaustive):

- Implementing good / best practice (whatever & however this might be achieved)
- Regular review and update (as required) of the 'Business Impact' (BIA) and 'Risk Management' analyses
- Ensuring all appropriate plans, procedures, processes etc. remain appropriate to the needs of the organisation (and particularly to its various [BC related] response teams)

Note: Just about everything in this Section **5.1** (and more) has been (or eventually will be) covered (in greater detail) in this guideline (i.e. the document you are reading now). It is also expanded upon ***to a lesser*** / ***limited degree***, in associated clauses of ISO 22313 itself

Section **5** / **2A** - **DO**

DEVELOPING the BCMS / **Understanding the Organisation** - (**BIA** / **RA** & more)

Some* BACKGROUND *Information

ISO 22313 / OPERATION / **Business Impact Analysis** + **Risk Assessment** etc. - 8.2

Note - before starting it is suggested that the serious reader reviews the appropriate Glossary terms found below (See [***separate*** document] CRPM Part 3 / Volume **1**):

- ✓ Activity / Activities
- ✓ BC Strategy
- ✓ BC (Tactical) Solutions / Treatments / Controls
- ✓ Business Impact Analysis
- ✓ Business Continuity Requirements - Resources Analysis
- ✓ Business Recovery / Business Recovery Plan
- ✓ Critically time-sensitive processes / activities + associated resources & dependencies
- ✓ Key Product / Service / Operation / Task etc.
- ✓ Maximum Tolerable Period of Disruption (MTPD) / Maximum Acceptable Outage (MAO)
- ✓ Minimum Business Continuity Objective (MBCO)
- ✓ 'Procedure' (and separately) 'Process'
- ✓ Recovery Time Objective (RTO)
- ✓ Risk
- ✓ Risk Appetite
- ✓ 'Risk Analysis' (and separately) 'Risk Assessment'
- ✓ Risk Category
- ✓ Risk Management
- ✓ Risk Treatments
- ✓ Stakeholder (+ Other Interested Parties) Analysis
- ✓ Threat

- Review 'Preamble Note 6' - starts page 36 of ***separate*** guideline document 'CRPM Part 3 / Volume **1**'
- Review 'BC at its Simplest' - page 20 of ***this*** guideline document
- Review the 'Note' (Understanding the Organisation) - page 53
- Review Section 4 / 1.5 - (Understanding the Needs & Expectations of Stakeholders / other Interested Parties) - page 72
- Review Section 4 / 1.6 - (Actions to Address Risks & Opportunities) - page 77

IMPORTANT: This section 5 / 2A provides ***background*** / ***introductory*** type material - re the BIA, RA etc. For the 'detail' see ***Section 5 / 2B*** (starts page 138)

Reminder: For simplicity, **ONLY MTPD** & **RTO** have been considered in this guideline. However, when / if planning BC strategy for recovery of **information and data** type assets, **MTDL** & **RPO** will additionally apply - and **MUST** be accounted for accordingly

Background Info - **Understanding the Organisation** (see also page *53* if required)

Introduction

An ***organisation*** achieves its 'purpose' by delivering its key products / services / operations / etc. (i.e. its '***business***' - whatever that might be) to ***customers*** (whoever or whatever they might be). Thus it is important that the organisation clearly ***UNDERSTANDS*** the (typically) adverse ***impacts*** (over time) that disruption / interruption of such key products etc. (together with their associated [*supporting / subordinate*] key activities) ***might*** have on such business, and (consequently) on stakeholders / other interested parties

It is also important to ***UNDERSTAND*** the associated inter-relationships / inter-dependencies and resource requirements of such *supporting / subordinate key activities* - and (in turn) the supporting / subordinate processes, procedures etc. - and (in turn again) the associated dependencies…………and so on

Furthermore, an organisation also needs to identify the ***threats*** (+ the associated ***vulnerabilities*** of business activities which such threats 'threaten') to its business, in order that it might adequately ***UNDERSTAND*** and ***'counter / control / solve / treat'*** (and / or possibly take advantage of [i.e. via 'risk appetite']) the ***impacts*** of same should they be realised. This latter is generically known as **'RISK MANAGEMENT'**

One (but only one of several) such risk 'counters / controls / solutions / treatments' involves the application of **BUSINESS CONTINUITY** type measures - **IF** appropriate so to do

Note 1 - In order to adequately achieve the above '***understanding***' requirements, an organisation needs to clearly identify and define its key products / services / operations etc. from the outset of the 'understanding the organisation' task

Note 2 - Generally speaking there are 5 'methods' of 'dealing' with ***threat*** related ***risk***. Four of them apply **before** the risk can occur, in order to try to ***prevent*** the risk 'realising' (actually occurring) in the first place. The fifth is deployed to manage the risk **after** it has actually occurred - otherwise known as ***business continuity planning*** (See figure 19 - page 176)

Note 3 - Apart from the ***BC related contex***t ***only***, **Risk Management** *typically lies outside the scope of CRPM Part 3 / Volumes 1 and 2.* (Reminder- you are reading Volume **2** right now)

Taking all of the above together, an organisation thus needs be able to identify and analyse such potentially disruptive ***impacts*** + their ***consequences*** (we shall see later in this Sub-section 5 /2 how this is achieved) to come up with a high level action plan (known as a **BC Strategy**) for how such consequences (if realised) might be dealt with - ***in the business continuity context***

Specifically, the organisation's person(s) responsible for introducing, implementing & maintaining a BCMS must acquire, retain, monitor, review and document the 'understandings' referred to above. He / she then ascertains how any potentially impacting threats might be dealt with (* *in the BC context only*) by application of appropriate BC measures (**'BC Tactical Solutions** - which meet the requirements of an associated BC Strategy

* Any other threats falling ***outside of*** the ***BC context*** obviously ***also*** need 'dealing with' i.e. within the ***Risk Management*** context. As already mentioned, this latter subject is outside the scope of this CRPM Part 3

Of course, the ***scope*** of the degree of understanding required is linked directly to the scope of the BCMS, as should be documented in an organisation’s *BC **Policy***. If e.g. ***only*** an airline’s ‘integrated operations control centre’ or an airport’s ‘baggage control system’ (i.e. both being ‘single’ business units for the purpose of this example) is required to implement a BCMS, then the breadth and depth of understanding required will be far less than that required for application of a BCMS to much or all of an entire airline; an entire airport etc.

If this process of ‘understanding the organisation’ is missed out, accomplished ineffectively etc. then the associated BCMS will simply not deliver what is required of it e.g. (list is ***not*** exhaustive)

- Threats & associated vulnerabilities (risks) to the continuity of operation might remain ‘undiscovered’ and thus not accounted for

- Appropriate and / or adequate BC strategy + associated tactical solutions + associated BC plans etc. might thus not be considered

- Appropriate and / or adequate BC related material resources might not be identified and thus available. Similarly, appropriate and / or adequate BC responders / teams (human resources) might not be available and - even if available might not be available in time - and even if available in time, might not be competent / experienced etc. to do what is required of them etc.

In other words, it is vital that this ‘understanding’ task be accomplished effectively and efficiently, documented and ***acted upon*** - before going any further with the BCMS project

How do we get to ‘understand of the organisation’?

1. By Involving the Most Appropriate Personnel

***The** ‘**Ideal**’ - in Theory*

Perhaps the best way to gain an overall & reasonably rapid ‘understanding of an organisation’ might be to assign appropriately skilled / experienced, ***middle level*** manager type staff to key BC positions (as a secondary duty i.e. ‘goes with the primary job’), right from the start (introduction) of the BCMS programme (there would also be other advantages in doing this of course)

Such managers (if chosen with care) should (collectively) ***already*** have a reasonably good understanding of how the organisation functions in general, simply as a result of ‘what they do’ during normal business. For example, in the aviation context, they might typically have backgrounds, knowledge and experience in e.g. Risk Management, Quality Management, Emergency / Crisis Response Management, Safety Management, Ops Control, Insurance, Procurement & Logistics etc.

The above might be supported in their BC roles and responsibilities by a seconded team of specific ’subject matter experts’ - drawn from those departments / business units which might be expected to be assigned future roles, responsibilities and accountabilities under the BCMS

Before commencing the project, all of the above mentioned staff (and others as required) should be provided with the required degree of BC competence & basic experience (e.g. via training & exercising - one or both possibly acquired ***externally*** if necessary) - together with the appropriate 'business tools', resources & support to 'do the job'

***The* '*Reality*'** *- in Practice*

In reality, just one (possibly two maximum) persons will typically be assigned ***primary*** BC roles, responsibilities and accountabilities within the organisation i.e. the appointed 'Business Continuity Manager' - together with the unlikely (???) possibility of a deputy / alternate

Furthermore, it is more than likely that this manager will be sharing his / her BC duties with some other concurrent role - typically risk; quality; emergency / crisis; safety etc.

However, it is expected that the BC Manager ***will*** identify (and request assistance from) the appropriate * middle level managers and subject matter experts (mentioned at the lower part of the previous page) and then further (ongoing throughout the BCMS life cycle) liaise and consult closely with them in order to achieve what is required to adequately 'understand the organisation' from the BC viewpoint

> * A note of caution here with reference to use of 'middle level managers' as referred to above i.e. it has been documented ***anecdotally*** that there is a tendency for some of such managers to possibly be '***averse*** (opposed) ***to change***' in general - whatever that change might be - including the potential and actual introduction and implementation of a BCMS into ***their*** 'organisation'
>
> Furthermore, there is the potential risk that such managers may be too inward looking and protective of individual spheres of interest to 'think outside of their own particular boxes'
>
> Both of these observations should be considerations when engaging middle level managers in the 'understanding the organisation' process. However, if handled correctly and sensitively, such potential problem areas (if any) might be overcome - thus permitting the desired, valuable and continuing contribution of such staff

The BC Manager - looked at from an aviation related context

If no BC Manager position(s) or equivalent (e.g. an airline's / airport's Quality or Safety Manager also 'doubling-up' as the BC Manager) already exists within the airline / airport etc. - then one (or more - remember that there should ideally be at least a deputy / alternate person too) should be created (with full top management backing; an outline approved budget etc.)

The introduction of BCMS should be deferred until an appropriate level of competence and skills has been achieved and demonstrated by the person(s) so appointed

Alternatively, an appropriate, external **AVIATION** related specialist BC consultant might be engaged to undertake the 'understanding the organisation' task - with the 'permanent' (designate) BC Manager (and deputy if there is one) closely understudying

Indeed, such external consultant will almost certainly be able to manage the ***entire*** BCMS introduction and implementation project him / her-self if so desired by the organisation, no doubt at some considerable financial cost!

IMPORTANT - The use of a (**NON-AVIATION background**) specialist BC consultant(s) **must** absolutely be avoided - for what are hopefully obvious reasons!

Another note of caution here which is aviation specific - i.e. whilst the number of ***general*** BC consultants around the world is growing rapidly, the expert / specialist ***aviation*** related BC consultant is still quite hard to find i.e. there are ***very*** few of them in the world and their number is typically ***not*** increasing

2. By Using the Most Appropriate * 'Business Tools'

* All systems, applications, controls, calculating solutions, methodologies etc. - used by an organisation to assist in better coping with e.g. changing markets, ensuring a competitive position in such markets, improving business performance etc. Use of same herein will typically be applied in a ***BCMS context***

When undertaking the 'understanding the organisation' task it has become 'standard practice' to use certain 'business tools'. The main ones are:

- **STAKEHOLDER** (+ other Interested persons) *Analysis*
- **BUSINESS IMPACT** *Analysis* (BIA)
- **RISK MANAGEMENT** *Analysis* (Assessment*)* (RA)
- *(BC Requirements)* - **RESOURCES** *Analysis*

Some ***overview*** level notes on these tools start just below. More detailed info on the design and application of the BIA and RA in particular can be found in Section 5 / 2**B** - starts page 138

Stakeholder / other Interested Party Analysis *- see also Section **4** / **1.5** (page 72) of this guideline*

This analysis is a useful starting point to 'understanding the organisation'

At its simplest, it might require a brainstorming session(s) with appropriate parties (possibly the middle level managers & subject matter experts already discussed in Section 4 / 2 .2 page 97) - to identify all (other) possible 'stakeholders / other interested parties' (internal ***and*** external) - associated with the organisation (in some appropriate way) ***in the BC context***

The latter are then placed in an ***initial***, listed ***order of importance*** (related to what they ***expect*** from the organisation and / or ***vice versa*** - such ***expectations*** being listed alongside the associated stakeholder / interested party - and so on, until the end of the list is reached)

The list is then used to assess the potential adverse impacts of significant (uncontrolled / non-specific) disruption on the organisation in general - as related to / in the context of each of the above ***listed expectations*** and, if necessary, the initial 'order of importance' on said list revised

The user / reader will recall that stakeholders / other interested parties can range from employees and shareholders - to legislators, regulators, customers and suppliers - to parent / subordinate organisations, the 'media', environmentalists etc.

Whilst 'customers' are typically expected to rate highly on the above list - there will be little choice other than to also 'highly' place legal and / or regulatory type stakeholders

Appropriate suppliers might also rate highly. For example, if defined aspects of an organisation's normal business (and thus business continuity) depend, in turn, on those of a listed supplier / suppliers - then the organisation must adequately account (in whatever way might be appropriate) for the business continuity capabilities / requirements of same

The importance of all forms of 'media' (including related 'public' use e.g. via social media etc.) should not be discounted, as it can and does exert a very significant influence on the 'public' and thus potentially, in turn, on the organisations concerned / involved. Airlines / airports etc. mishandling a 'major disruption to business' type event can expect a hard time from TV, newspapers, electronic (social) media, the public etc. - including consequent, adverse impact on brand, image and reputation - perhaps to the extent of the organisation(s) involved being in danger of 'going out of business'

Pressure groups can (and have in the past) halted the building and / or expansion of airports and can influence e.g. an airline's environmental policy, with inevitable financial & operational (and perhaps reputational) consequences (think 'Greenpeace' and similar activist groups)

Finally (and a major reason for undertaking this particular analysis) the information acquired is used to assist in ***identifying*** and ***prioritising*** (scoring by degree of urgency with regard to continuity / recovery of operation) the organisation's ***key products*** / *services* / *operations* (together with the latters' associated ***key main*** and ***key supporting*** activities + their associated processes, procedures, inter-relationships, inter-dependencies, resource requirements etc.)

Business Impact Analysis (BIA)

Note - the context, scope, methodology (how to do it) and measurement / assessment criteria of / for the ***BIA*** should be defined, agreed to (by top management) and documented in advance. '***Consequence categories***' and '***impact criteria***' (see from bottom of page 149 to page 155) should be chosen and standardised (insofar as is possible / practicable) between the BIA and the RA - thus providing a degree of desired consistency between them ………… more on this can be found in Section 5 / 2B (starts page 138)

General

BIA (when taken together with the other three components [business tools] of the 'understanding the organisation' process) is the 'foundation' of Business Continuity Programme Management. In brief it (the BIA) is all about:

- Identifying an organisation's ***key product****(s) / services / operations* etc.

- * Identifying *key* ***main*** *activities* (internal & external) associated with delivering the above key product(s) / services / operations

- * Identifying *key* ***supporting*** *activities* (internal & external) associated, in turn, with delivery of the above key main activities

Connects to '***key product**(s) / services / operations*' etc. bullet point - near bottom of previous page

- * Assessing the ***maximum***, anticipated degree of ***overall***, adverse ***impact*** of disruption / interruption on ***each*** identified *key **main** activity* - as related to delivery of the associated ***key products** / services / operations*

  'Score' the results from above in 'units' of ***impact assessment*** (for ***eventual*** input into the ***risk management*** [assessment] matrix [see examples in figures 11 to 17, pages 157 to 165]) **+ also** in terms of 'priority for action' (e.g. 'highest', 'high', 'medium', 'low' or 'for possible future attention') ……………and (+)

Before looking at pages 157 to 165 it is ***IMPORTANT*** to read the associated notes - starting bottom of page 155 & finishing page 156

- * Assessing the ***maximum***, anticipated degree of ***overall***, adverse ***impact*** of disruption / interruption on ***each*** identified *key **supporting** activity* - as related to delivery of the associated *key **main** activities*

  'Score' each result from above in 'units' of ***impact assessment*** (for ***eventual*** input into the ***risk management*** [assessment] matrix [see examples in figures 11 to 17, pages 157 to 165]) **+ also** in terms of 'priority for action' (e.g. 'highest', 'high', 'medium', 'low' or 'for possible future attention') ……………and (+)

  * ***Reminder*** - The term '***activity** / **activities***' (as used herein) typically relates to a series of associated ***PROCESSES* -** which are, in turn, made up of associated ***PROCEDURES*** etc. For the sake of simplicity, brevity etc. the latter two have been ignored here

  However, when conducting a BIA for real, **ALL** such ***processes*** (as associated with each key ***main*** activity **+** each key ***supporting*** activity) and all such ***procedures*** etc. (as associated with each, ***parent*** process……….and so on) **MUST** be similarly accounted for as per above - and assigned MTPDs, RTOs and MBCOs (see Glossary if necessary) ***in their own right*** where appropriate (in the same manner as described just below) - and the results documented accordingly

- Estimating & applying associated ***MTPDs*** based on the results of the above - as appropriate ……………………and (+)

- Estimating & applying MTPD associated (***initial estimate***) ***RTOs*** based on the results of the above - as appropriate ……………………and (+)

- Identifying 'internal and external dependencies / inter-dependencies' etc. - relating to the above 'key ***main*** activities' and 'key ***supporting*** activities' and, where appropriate, ***adjusting initially estimated RTOs*** *(as calculated just above)* to adequately account for same ……………………and (+)

- Setting the minimum level of operation (***MBCO***) to be achieved when a disrupted activity is assumed to 'resume' at said RTOs ……………………and (+)

- Identifying any *'single points of failure'*......................and (+)

- Using ***impact assessment*** ('scores') from further above as partial ***inputs*** to the ***associated risk management*** *(assessment)* process ....and (+)

- ***Pulling together & documenting*** the results of all the above into a report - the outcomes of which, (when combined with the results of the other 3 components [business tools] of the 'understanding the organisation' process [as approved by top management]) ** **MIGHT** be used to formulate a ***'BC Strategy'*** ....and (+)

  ** It is possible that some / all of the above results indicate that BC type measures are ***not*** chosen to mitigate etc. a particular risk (i.e. ***other*** **RM** measures might be used instead). In this guideline we are, of course, assuming that BC type measures ***are*** chosen / used

  Note - The ***BC Strategy*** outlines (from the higher level BC viewpoint) what the organisation needs to achieve going forward from the 'understanding the organisation' task (see bullet point list just below for some examples). This is necessary to try to ensure continuity of its key activities etc. (in the BC context only), following a significant disruption event to same

  - Formulation of associated '**BC Tactical Solutions** / Treatments / Controls etc.'
  - Setting up of an '**Incident Response Structure**'
  - Production of the associated **BC plans & associated procedures** etc.

- ***Identifying and accounting for other activities / processes*** which ***might*** also require eventual consideration from a business continuity context - but which are ***not*** expected to require application of the ***formal*** BIA process described above

It can be seen that the BIA necessarily focuses on those activities - *** failure of which would most quickly threaten whatever it is that needs to be delivered / produced / operated etc. This focus is typically directed to 'operational / high profile / up-front' activities (key ***main*** activities - both internal and external) - ***particularly*** (for most organisations) ***those which create revenue***

We now also know that many (if not most) key main activities will depend, in turn, on the continued operation of associated 'backroom' activities (key ***supporting*** activities - both internal and external) which **must** also be analysed via the BIA. Associated ***processes*** and ***procedures*** etc. must also be accounted for / considered (see 'reminder' on previous page)

*** The BIA typically works on a worst case scenario e.g. assuming the impact of a significant disruption event on a particular activity - might ***eventually*** (if nothing was done) lead to the latter's ***cessation***

The BIA can be difficult to perform competently - but it is important to 'get it right'. It can also take considerable time and effort to complete - depending on the size and / or complexity of the organisation, the scope of the BIA, the co-operation of participants and resource providers (including budget) - together with the competence / experience / availability etc. of the person(s) undertaking the associated data gathering and analysis etc. of same

Seasonal / Calendar Variations

Within the BC context a further application of ***time*** (e.g. additional to MTPD and RTO) must also be considered i.e. certain key activities etc. become more time-sensitively critical (more urgent and / or of higher importance) at certain times / dates of the year e.g.

- Aircraft and crew increased availability requirements at peak travel / vacation periods
- Ensuring sufficient funds are available to pay staff on payday
- Ensuring that airports have adequate de-icing arrangements in place during periods where same are expected to be required (same goes for snow / ice clearance ops) etc.

Additionally, there may be key projects etc. which must be delivered on time and, if disrupted, will have serious consequences (whatever they might be) for the organisation

> Within the BC Planning context (and thus applicable to the 'understanding the organisation' task) - the assumption is typically made that 'disruption' to 'whatever' occurs at the ***worst possible time*** - as associated with such seasonal / calendar variations

Single Point(s) of Failure

It is particularly important that a BIA attempts to identify activities involving *'single points of failure'* (SPOF) - for example:

- a single person (in a small airline) maintaining the entire on-board aircraft documentation set - as required to conduct public transport flight operations
- an airline using a single in-flight catering supplier at its main / hub base (with no alternate supplier provided for)
- a major airport using just one type of navigational guidance aid to its main runway(s)
- an airline / airport / GHA etc. using a digital telephone system with no analogue telephone system backup
- ICT servers having no off-site backup capability; insufficient bandwidth / capacity etc.

Scope

In addition to looking at the ***internal*** scope of a BIA, it is important to ensure that the BIA extends outside of the organisation where required - e.g. suppliers, legislators / regulators, insurers, competitors etc. Diligent completion of the *'Stakeholder / other Interested Parties Analysis'* should ensure that this matter is adequately accounted for

Pre-emptive & Retrospective BIAs

It might be advantageous to complete a '***first try***', simplified BIA (i.e. during the planning / preparation phase as per Section 4 of this guideline) ***before*** doing almost anything else - as so much (following afterwards) depends on it e.g. BC Policy - including the scope of the BCMS etc.

A further (updating and more formal) BIA (as described here) would then be held later

BIA derived data / information can also be used ***retrospectively*** e.g. to possibly revise previously decided matters (e.g. the ***initial*** BCMS ***scope*** and ***initial*** estimates of ***resources*** required - as documented in the organisation's 'first try' BC Policy document) for which appropriate BIA derived material might not have been available at such (earlier) time

BIA Outputs

To recap, BIA results, when 'combined' with the results of the ***other*** three 'business tools' used in the 'understanding the organisation' process (particularly the ***risk assessment*** - see page 130) will directly influence which (if any) ***BC Strategies*** (and thus, in turn, which associated ***BC 'Tactical Solutions*** / *Treatments etc.'*) are finally chosen for implementation - and will also be used to assist in the eventual formulation of the associated ***BC Plans*** (including all required ***procedures***) and the set-up of the ***Incident Response Structure*** (BC and business recovery aspects ***only*** for latter) - as required by the organisation

See Section **5 / 3** (p. 197) & Section **5 / 4** (p. 223) for more info concerning 'BIA Outputs'

Time-Sensitive Activities

The above sub-title relates to a priority ranking system for an organisation's key main and key supporting etc. activities / processes etc. (as appropriate), the loss of which is * usually (but not always) proportional (typically in the form of 'adverse impact') - to the '***time***' for which they remain unavailable'

* Note that some activities will earn their place at or very near the top of such a priority list due their nature (i.e. ***regardless of the time*** for which they are unavailable) e.g. those affecting the safety of life; breach of legal / regulatory matters; very high financial impact etc.

As an example of what the above means in practice - take two important airline activities - such as the operation of its main (only) '***call*** / ***contact*** / ***information*** / ***reservations centre***' - and the provision of '***in-flight catering***' for its flights

Let's now assume that ***both*** activities are seriously and simultaneously disrupted by a 'crisis' event (whatever that might be) - and that 'time to recover' is a significant factor (which it really would be of course - for both activities)

Without a call centre, no calls can be made / received - thus no (or extremely reduced) business gets done - thus very significant ***adverse*** customer service and financial etc. implications can quickly arise. This, in turn, can lead to potentially adverse impacts on brand, image and reputation and the 'bottom (financial) line' - which, if serious enough, could put the airline out of business - at least temporarily and possibly permanently. (Note: For the purposes of clarity / simplicity internet only bookings etc. have been ignored in the above example. However, even if accounted for [as available] the contrast with 'in-flight catering' would still be relatively valid)

Conversely, the in-flight catering disruption is relatively 'low key' in terms of adverse impacts, in that a range of effective ** ***BC tactical solutions*** / *treatments* (see bullet point list below) are typically (and relatively quickly) available:

** Providing an easily & rapidly ***outsourced*** (basic) food service such as sandwiches and snacks

** Providing cash ***vouchers*** for use at the departure airports' food outlets

** Ensuring airports' food outlets are ***adequately stocked & re-stocked*** throughout disruption

** Ensuring airports' food outlets ***remain open*** for the required periods

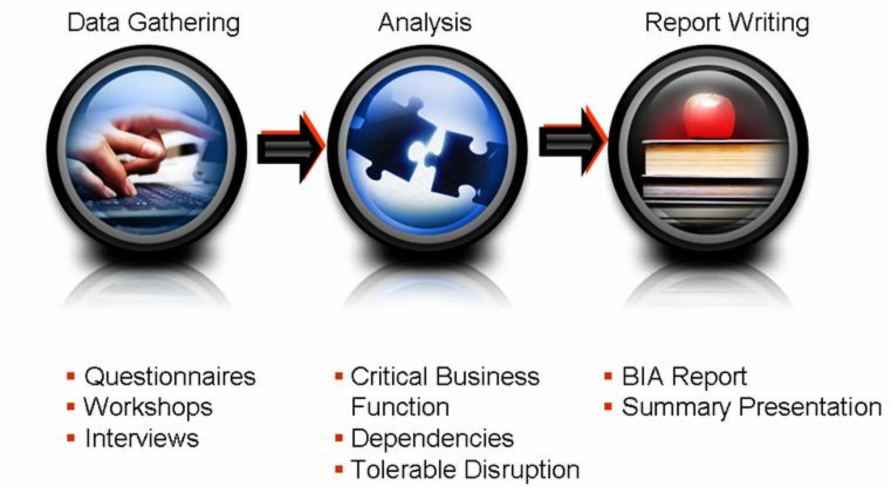
** Requesting ***customers to provide own basic food*** e.g. sandwiches & snacks

** Arranging appropriate and adequate ***compensation*** and / or ***incentives*** etc.

It is clear that the **MTPD** (and thus, in turn, the associated **RTO**s) calculated for the call centre must be very short - whilst those for in-flight catering might be commensurately longer

When combined with a good communications service (with stakeholders / other interested parties - particularly passengers), the obvious result should mean the airline positioning an in-flight catering disruption at a ***significantly*** ***lower*** BC ***priority*** response level in terms of ***time*** - than that of the call centre

The BIA process might be summarised (***VERY*** simplistically for now) as follows:



***Risk Management** (Assessment)* - **RA**

Note 1 - the context, scope, methodology (how to do it) and measurement / assessment criteria of / for an **RA** should be defined, agreed to (by top management) and documented in advance. In particular, '***Consequence** / **Impact Categories***' and '***Impact Criteria***' (see pages 149 to 155) should be defined and standardised (insofar as is possible / practicable) between the RA and the BIA - thus providing the degree of desired consistency between them .... more on this in Section 5 / 2B

Note 2 - most BC concepts, associated 'literature' and practitioners refer to '***risk assessment***' as being part of the 'understanding the organisation' process. Pedantically speaking, however, the term we should be using instead is 'risk management' - of which 'risk assessment', 'risk analysis' etc. are just sub-component parts - (see Glossary in [separate document]) CRPM Part 3 / Vol 1 - for more details)

Introduction

'Pure' risk management is the practice of systematically identifying & understanding risks to an organisation + the controls / solutions etc. that are (or eventually will be) put in place to 'manage' them. Ultimately the process gets to the point of deciding whether (as related to a specific business activity / function etc.) a risk is acceptable .... or requires further action to mitigate (reduce and / or otherwise manage [e.g. even avoid in extremis]) its (typically adverse) potential impacts ***and / or*** likelihoods of occurrence

The risk management process is typically designed so as ***not*** to encourage organisations to be risk averse. On the contrary, it can provide organisations with a degree of confidence re 'managing' risk to an acceptable level and to ***take on*** a level of risk commensurate with 'opportunity' (i.e. risk tolerance / appetite) where appropriate. The key element in managing risk is to adequately / sensibly balance 'risk and reward' opportunities

A 'risk averse' culture within an organisation can create inflexibility and put barriers in the way of achieving the organisation's business objectives. In contrast, the unthinking acceptance of disproportionately high risk can have significant, adverse impacts

From the BC viewpoint, risk management techniques **EVALUATE** the ***probability / likelihood*** (estimated likely frequency / rate / chance of occurrence) and estimated / predicted * ***impact**(s)* of ***specified threats*** - which could potentially cause disruption / harm etc. to an organisation's key product / services / ops etc. (via disruption / harm to the latters' associated key main and key supporting activities etc.) - should such threats actually occur (be realised)

* Note - pure risk management (i.e. with ***no*** BC association) works out its own ***impact*** levels from a process ***similar*** to that of the BIA. However, risk management inputs into ***business continuit***y operations typically take their impact levels ***from those found during the associated BIA***

The above evaluation is typically facilitated using a 'Risk ***Probability*** vs Risk ***Impact*** Matrix' (see figure 8 - page 132) - in order to eventually assess choices and application of the available *risk treatments / controls* (see second bullet point ***list*** on next page) - necessary to reduce (or even avoid) the ***likelihoods*** .... and / or mitigate (reduce) the ***impacts*** of realised threats

Each identified and prioritised (i.e. prioritised in terms of what needs to be addressed first, second, third etc. in order to ensure continuity) key main activity and key supporting activity etc. (produced as an ***OUTPUT*** of the **BIA** process) is subjected, in turn (as an ***INPUT***), to the **RISK** management (assessment) process

The BIA provided inputs to the RA matrix are:

- The details of the specific activity which is to be risk managed (assessed)
- Parameters for ***one*** arm (side) of the risk assessment matrix i.e. the degree of adverse '***impact***' expected should the threat under consideration actually occur (be realised)

The '***likelihood / probability***' of the particular risk occurring to the specific activity (an ***OUTPUT*** of the risk management [assessment] process) forms the ***other*** arm of the RA matrix

Based on study / analysis of the resulting matrix, appropriate 'risk treatments / controls / solutions' are formulated to 'manage' the particular risk in question

Such risk treatments etc. typically comprise the following - any / all of which may be applied concurrently or not at all, depending on the nature of the risk, the organisation's business model and risk appetite, the results of a costs / benefits analysis (does the cost of the treatment outweigh the benefits?), impacts on users, effort required, scope of the RA etc.

- ***Transfer*** and / or share the risk e.g. through insurance, third parties (e.g. codeshare / alliance partners - in the case of airlines) etc.
- ***Accept*** the risk (do nothing) e.g. where impact / probability outcome is acceptably low; when the outcome lies within the organisation's current risk appetite parameters etc.
- ***Avoid*** the risk - abandon activities (or, even better, don't start them in the first place) giving rise to unacceptable risks and / or remove cause(s) of the risk(s)
- ***Reduce likelihood*** (probability) of risk occurring
- ***Reduce impacts*** of realised risk i.e. plan to 'solve / treat / control' the risk ***AFTER*** it has actually occurred, typically by using ***BC*** and *'other measures'* (emergency / crisis response planning & business ***recovery*** operations [in contrast to business ***continuity*** operations] being examples of the latter')

Note that the risk treatments identified in the first four bullet points immediately above are 'pre-emptory' i.e. they are applied ***before*** any potential threat can be realised

The last bullet point (using BC and similar measures) is the only risk treatment typically applied ***after*** the threat has been realised - and also the only treatment which has significant ***time*** (i.e. ***MTPD*** and ***RTO***) and performance / output etc. (i.e. ***MBCO***) considerations to account for

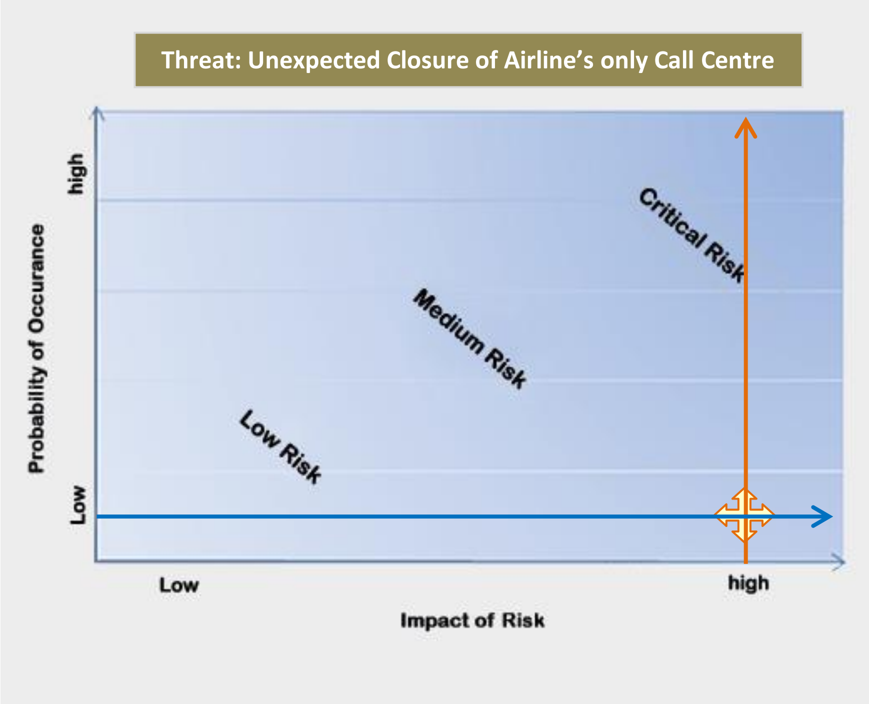


Figure **8** - Simplified example of a ***very*** basic Risk Matrix

Note 1 - the adverse ***impact*** (of the threat occurring) in the example above is rated as high and its ***probability / likelihood*** as low. In such circumstances such risk would probably be ***acceptable*** to the airline, ***provided*** that it is capable of being actively managed (mitigated) as a * ***high priority*** requirement - and by having the freedom to apply the most appropriate ***risk*** treatment(s) / controls (remember that ***one*** such risk treatment / control is to apply ***BC solutions*** / treatments / controls ***after*** the risk has actually occurred)

* Comment - 'high priority' status is necessary for this ***particular*** 'call centre' example due the critical nature of the activity (assuming e.g. that it is the airline's ***only*** call / contact / reservations centre) and the potentially high adverse impacts should the threat be realised. In contrast, if the 'provision of ***in-flight catering***' was e.g. the activity being risk assessed above, the 'adverse impact' effect would be considerably lower, whilst the 'probability' effect might typically be low or almost low overall. The risk of the latter to the airline would also be acceptable and would also need to be treated / managed. However, it should neither receive the same priority for treatment (nor the same degree / extent / expense of treatments) as the call centre example

If it is not possible to actively manage the particular risk as described - 'avoidance' should be considered. The most obvious way to achieve this is to stop the activity (or not start it in the first place)

At a simplistic level, the following 'priorities for action' to be taken relate respectively to 'high', 'medium' and 'low' risk management (risk assessment) results:

High Priority Action (**H**) - Implement highly robust solutions as soon as possible

Medium Priority Action (**M**) - Implement robust solutions within a reasonable timeframe

Low Priority Action (**L**) - Accept the level of risk and / or………… implement basic solutions at some appropriate, future time

Note 2 - examples of ***risk treatments*** which can be applied ***before*** a risk occurs (e.g. in the call centre scenario used in the matrix on the previous page) might typically include:

- Installation of an uninterrupted / no-break power (electrical) supply system
- Installation of a sophisticated fire warning and suppression system
- Instant availability of an analogue telephone system (complete with analogue compatible telephones) to back up what will almost certainly these days be the primary method of telephone communications with customers / clients i.e. via a ***digital*** telephone exchange
- Very rapid access to a backup system for the software used to manage call centre operations
- Cross-training between the managers and operators of the different call centre functions e.g. customer services versus reservations versus 'loyalty' (frequent flier) etc.
- Establishing appropriate security to prevent unauthorised access to call centre facility (e.g. by terrorists; by environmentalists etc.)
- Establishing a very robust ICT security system

Examples of pre-planned and pre-prepared ***risk treatments*** which can be applied ***after*** the risk has realised (**NB:** these are known as ** **BC tactical solutions** / treatments / controls and might include [for the same scenario used just above]):

- Very rapid activation of a 'hot' alternate facility (e.g. many larger airlines operate several call-centres typically dispersed around the world in geographically dispersed locations. This is typically done for commercial purposes but would obviously also benefit a 'business continuity' type situation)
- Use mobile / smart phones (permanently on charge), email, social media and other manual workarounds. (Mobile phone and email contact info publicised via airline's main website)
- Work from home i.e. some type of 'virtual call centre'
- *** Use an outsourced (external / independent) commercial call centre service

** - the use of BC Tactical Solutions / Treatments etc. will be covered in Section **5 / 3** (starts page 197) of this guideline

*** - this particular option requires staff at the outsourced call centre to have an adequate level of pre-established competence and experience already in place - together with access to the appropriate, operating software. Whilst this option ***can*** work, it would typically be expensive!

Reminder - 'pure' **risk management** is ***only*** concerned with potential risk ***likelihood*** & ***impact*** factors

However, we also need to consider the ***time*** dimension when using *risk management* **in the *BC context*** i.e. efforts spent on implementing ***BC related*** risk treatment measures should be ***first targeted*** on those key operations / activities etc. - which will ***most quickly*** have an adverse ***impact*** on the organisation - if significantly disrupted

Reminder - do not confuse '***risk***' with 'consequence' e.g. 'injuries', 'financial loss' and 'reputation damage' etc. - are ***not*** risks……………………….they are ***consequences*** of realised risk

See Section **5** / 2B / 3 (starts page 167) for more detailed info on the RA process itself

Who is Responsible for Risk Management (within the organisation?)

Where an organisation does ***not*** already have a 'risk management' (RM) department / business unit / manager / plan etc. - ***top management*** should decide where (in the organisation) such RM responsibilities will lie - and take appropriate action for them to be fulfilled

Whilst it is undoubtedly desirable for the larger and / or more complex organisations (such as many airlines, airports & GHAs) to have ***separate*** emergency / crisis response planning, business continuity planning and risk management business units (with separate managers for each) - this will not be practicable / possible / feasible in many cases

However, it is strongly recommended that top management does ***not*** consider assigning all ***three*** accountabilities to a single person - as this simply will not work in practice

Exceptionally*, an incumbent and* **very capable** 'emergency / crisis response planning manager' might be considered suitable for taking on additional BC accountabilities. Same principle goes for an incumbent risk manager; quality manager etc. - i.e. such persons would be assuming ***two*** concurrent accountabilities

However, in circumstances where (relatively rarely) airlines, airports etc. do have a large emergency / crisis response (or similar discipline) business unit (say 4 to 5 persons) - then it may be reasonable for the Emergency / Crisis Planning, BC and Risk accountabilities to be operated by such single unit (provided appropriate competencies, skills, experience, resources, rewards etc. are established and maintained)

Lastly, the International Civil Aviation Authority (ICAO) requires what may be termed the 'operational safety elements' of aviation related organisations (i.e. the appropriate departments / business units of airlines, airports, ground handling operators, aircraft repair and maintenance operators, flight training operators - even entire countries [states]) …………… to comply (mandatory) with the requirements of its (ICAO's) 'safety management system - **SMS**' programme

(Safety) ***Risk Management*** (SRM) forms a significant part of the latter ***SMS***. Accordingly, it is more than likely that for many aviation related organisations, a fair degree of risk management work (including risk analysis / assessments) ***will have already been completed*** regarding 'operational safety' matters - typically accomplished by e.g. the organisations' safety business units

The above information will obviously be of ***some*** use for BC (Understanding the Organisation) purposes - at least in the area of (aviation risk related) ***operational*** safety

However, do remember that aviation related BC also applies to many matters which fall outside the ICAO SMS scope. Such matters must still be accounted for by the organisation of course - using 'traditional' risk management techniques (which includes use of BC measures [where appropriate])

The (BC Requirements) - Resources Analysis

See ***also*** resources related information found in Sub-sections **4 / 1.9**; **4 / 2** and **5 / 3.5** of this guideline

Part 1

Concurrent with the 'understanding the organisation' task it is necessary to also look at the business continuity requirements in terms of the ***resources*** available to / required by the organisation, in order to resume disrupted key product / services etc. (together with associated key main and key supporting activities [+ the latters' component processes procedures, interdependencies] etc.) to pre-defined levels (MBCO / MAO) within pre-defined timescales (MTPD / RTO)

The purpose of this analysis (at this particular time) is to collect ***initial*** / ***outline*** ('educated best guess' if necessary) information on the types and quantities of resources (e.g. people, technology, facilities, data / information, supplies etc.) potentially required for resumption and continuance of those activities described in the para above. The analysis should also account for any additional resources required e.g. to operate workaround solutions; clear work backlogs etc.

This analysis is then used to ***contribute*** to the * ***more specific and comprehensive*** resource information required - when eventually determining '***BC Strategies***' and the establishment of associated '***BC Tactical Solutions*** / Treatments / Controls etc.'

* See also Sub-section 5 / 3 / 5 (page 215) - BC Strategy - '***Establishing Resource Requirements***'

Note: - if the above is going to be accomplished more thoroughly at some future time (which is typically how it works in practice i.e. ISO 22313 accomplishes this in clause 8.3.3 as part of formulating BC Strategy) the serious reader might be wondering why we are wasting time and effort making an 'educated guess' at it now, in the 'understanding the organisation' phase?

The answer is assumed to be that when the 'understanding the organisation' reports are presented for sign off by top management - the latter needs to be aware of ***all*** of the implications (particularly as they relate to ***potential budget*** and ***assignment of other resources*** - especially people) before committing to action (and spending money!)

Part 2

The organisation should understand the threats to and vulnerabilities of the resources required by its activities etc. - particularly those with high priority and / or with a significant (replacement) lead-time etc.

Understanding the Organisation - *a Pictorial Summary*

Figure 9 (see next page) attempts to diagrammatically portray a simplified 'understanding the organisation' type task, up to and including the selection of appropriate ***risk** solutions / treatments*. It further indicates that ***one*** *(but only one of five)* of the risk treatments available (i.e. 'reduce ***impact****(s)*' - ***only*** chosen ***if appropriate*** to the results of the 'understanding the organisation' task) relates to the use of appropriate and associated ***BC** measures*

Reminder - the latter ('appropriate and associated BC measures') are ***managed*** by the setting of an associated '***BC Strategy***' - and ***implemented*** by selection of the most appropriate tactical 'measures' etc. available - (otherwise known in this guideline as '***BC Tactical Solutions*** / *Treatments / Controls*')

To complete this 'big picture' beyond the 'understanding the organisation' aspects - the diagram also indicates the further, required developments of the BCMS - which will be covered later in this guideline i.e.

- Establishing an ***Incident Response Structure*** (IRS) and capability
- Producing ***Business Continuity*** & ***Business Recovery*** Plans - including associated procedures
- Cyclically ***exercising*** the BCMS
- Cyclically (and / or as required) ***maintaining***, ***reviewing***, ***evaluating and continually improving*** the BCMS

The user / reader will note from figure 9 that the * BIA and RA appear to be completed at the same time. This has been shown in this way for the purposes of simplification

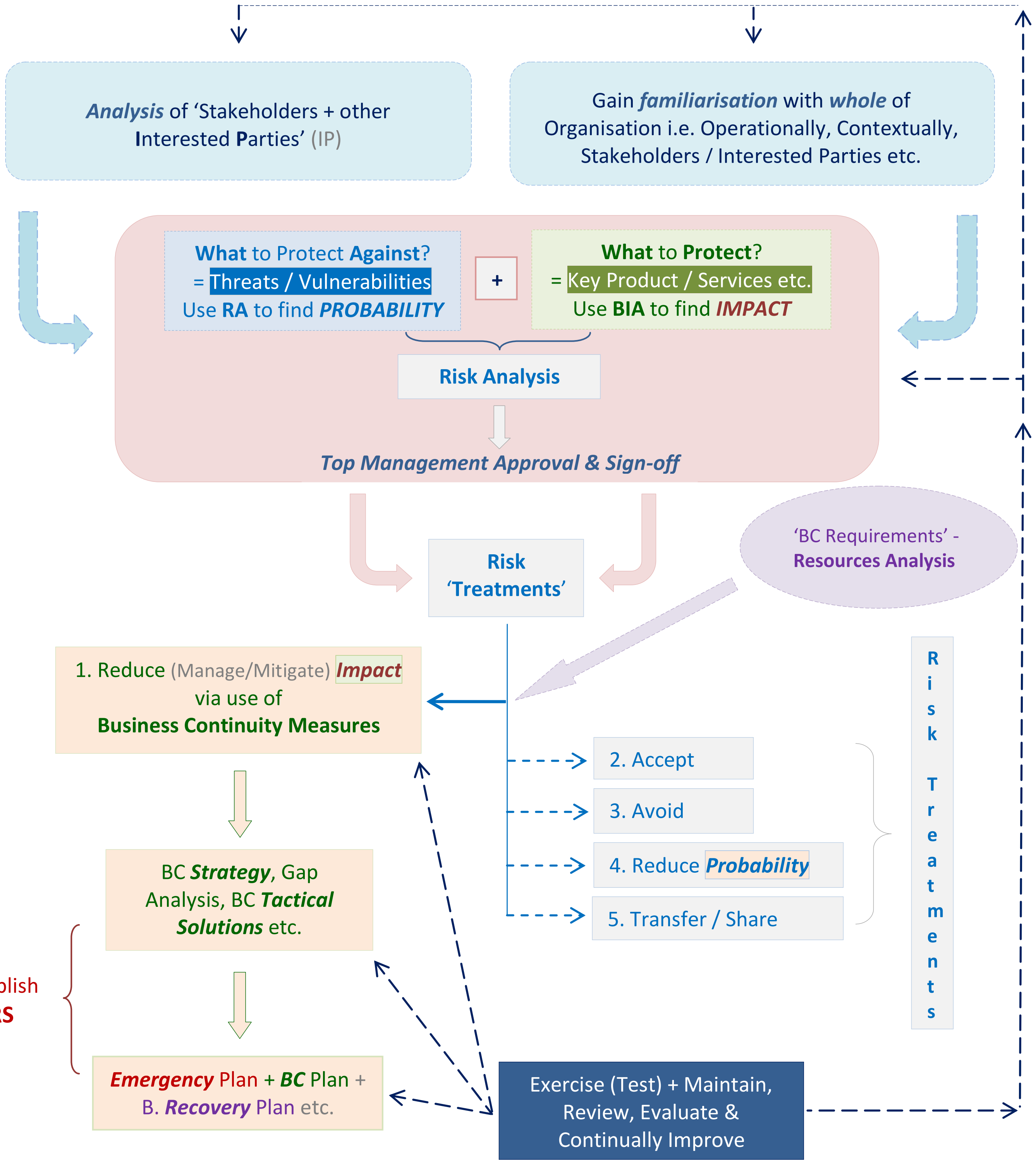
*** In *this* guideline the *BIA* is addressed first before we move on to complete the *RA*. There is, however, no reason why this sequence cannot be changed. There are advantages and disadvantages to both but, if completed correctly, the end result should be the same for any set of given circumstances**

There are, however, possible efficiencies to be made if the BIA and RA ***are*** conducted concurrently. This is because the same subject matter experts providing input to the BIA are almost always the same persons providing input for the RA

However, it is recommended that such 'merging' is used only for the simpler / less complex organisations ***OR***.................... in circumstances where the person in charge of the 'understanding the organisation' task is justifiably ***very*** confident that both can be conducted concurrently without detrimental consequences

Reminder - Most ***aviation*** related organisations will have already completed ***some*** of the risk related work required in the 'understanding the organisation' task - as per the boxed information (last 4 paras) on page 134

Where the aviation related organisation is fortunate enough to have a dedicated 'Risk Management' department / business unit - it is reasonable to assume that all ***risk management*** related work associated with ***BCMS*** implementation & operation - will be handled by same. ***It would be ideal*** *(and common sense)* ***if they also covered Business Continuity matters***!!!



Analysis of 'Stakeholders + other Interested Parties' (IP)

Gain *familiarisation* with *whole* of Organisation i.e. Operationally, Contextually, Stakeholders / Interested Parties etc.

What to Protect **Against**?
= Threats / Vulnerabilities
Use **RA** to find ***PROBABILITY***

+

What to **Protect**?
= Key Product / Services etc.
Use **BIA** to find ***IMPACT***

Risk Analysis

Top Management Approval & Sign-off

Risk 'Treatments'

'BC Requirements' - **Resources Analysis**

1. Reduce (Manage/Mitigate) ***Impact*** via use of **Business Continuity Measures**

2. Accept

3. Avoid

4. Reduce ***Probability***

5. Transfer / Share

Risk Treatments

BC ***Strategy***, Gap Analysis, BC ***Tactical Solutions*** etc.

Establish **IRS**

Emergency Plan + ***BC*** Plan + B. ***Recovery*** Plan etc.

Exercise (Test) + Maintain, Review, Evaluate & Continually Improve

Figure 9 - ***Understanding the Organisation*** i.e. → IP Analysis → BC Requirements Resources Analysis → BIA → RA → Risk Treatments → BC Strategy → BC Tactical Solutions → BC Plans & Procedures ………………… → IRS ← Exercise (Test), Maintain, Review, Evaluate & Continually Improve

Section 5 / 2B - DO - DEVELOPING the BCMS

Understanding the Organisation - (BIA / RA & more)

ISO 22313 / OPERATION / **Business Impact Analysis** + **Risk Assessment** etc. - 8.2

The Analyses - in a little more Detail

Note 1 - it is important that users / readers clearly understand that what follows in Sub-section 5 / 2B is provided at a 'bird's eye view' (overview) level only e.g. the ***BIA*** and ***RA*** alone for a medium to large sized organisation can take months to plan, implement and complete (depending on the organisation's business; BIA / RA scope etc.). The task can also be quite complex in certain circumstances

Whilst what is provided herein is essential information by way of understanding the associated processes etc. at said 'overview' level - further guidance will be required in reality - unless the user / reader is ***already*** competent and experienced in the appropriate ***RM*** (including ***BC***) matters

There are quite a few resources available to at least address the '**competence**' requirements mentioned above (via internet; books; by taking commercially provided training etc.) - almost all of which * require purchase / payment

* ***You are reading the exception to this right now!*** A reminder also that ISO has produced its own (separate) guide on the subject of BIA (ISO / TS 22317:2015 - BIA [$138 USD for 27 pages!!!]) which, as you will note, requires additional purchase over and above the costs of ISOs 22301 and 22313

The '**experience**' requirements will need to be gained / earned in the usual way i.e. hands on familiarisation (including 'exercising') over a suitable period of time, under the watchful eye of someone who already has such appropriate competence, experience and (preferably) qualification

If unfamiliar with the 'understanding the organisation' concept, a review of pages 120 - 137 (of this guideline) is strongly recommended. See also the limited reference material - pages 193 to 195

Note 2 - concerning what is to follow, the organisation's ***top management*** should ensure that:

- Sufficient time, preparations and resources are allocated to / for the required tasks
- The context, scope & methodology (how to do it) of / for performing the tasks have been pre-set, approved, financed, documented and will be reasonably followed
- Appropriate measurement (evaluation) criteria related to the tasks have been set, approved, documented and will be reasonably followed
- Staff undertaking the tasks are appropriately skilled / experienced / competent / qualified
- Staff / others required to respond to task requirements e.g. via workshops, interviews, questionnaire completion etc. - will make themselves appropriately available and 'co-operative', as required

Reminder *- for simplicity,* **ONLY** ***MTPD*** & ***RTO*** *have been considered in this guideline document. However, when / if planning* ***BC measures*** *etc. for recovery of* ***information*** *and* ***data*** type assets, **MTDL** & **RPO** *will additionally apply - and* **MUST** *be accounted for accordingly*

Section 5 / **2B** / **1**

Stakeholder / other Interested Parties Analysis

The method of accomplishing the ‘stakeholder / other interested party’ analysis has already been adequately described in Section 4 / 1.5 & Section 5 / 2A - and is thus not repeated here

Section 5 / **2B** / **2**

Business Impact Analysis

Firstly, it is advisable to refresh again on the meaning of the terms:

- *‘Minimum Business Continuity Objectives* (MBCO)*’*
- *‘Maximum Tolerable Period of Disruption* (MTPD)*’*
- *‘Recovery Time Objective* (RTO)*’*

Refer to the Glossary section (of separate document CRPM Part 3 / Vol 1) if necessary

A review of figure 10 on the next page is also recommended in order to better understand the relationships between some of the main terminologies used - as related to the BIA task:

Note: The BIA typically works on a worst case scenario e.g. assuming the impact of a significant disruption event on a particular activity - might eventually lead to the latter’s ***cessation***

As mentioned, the BIA can be difficult to perform competently - but it is important to ‘get it right’

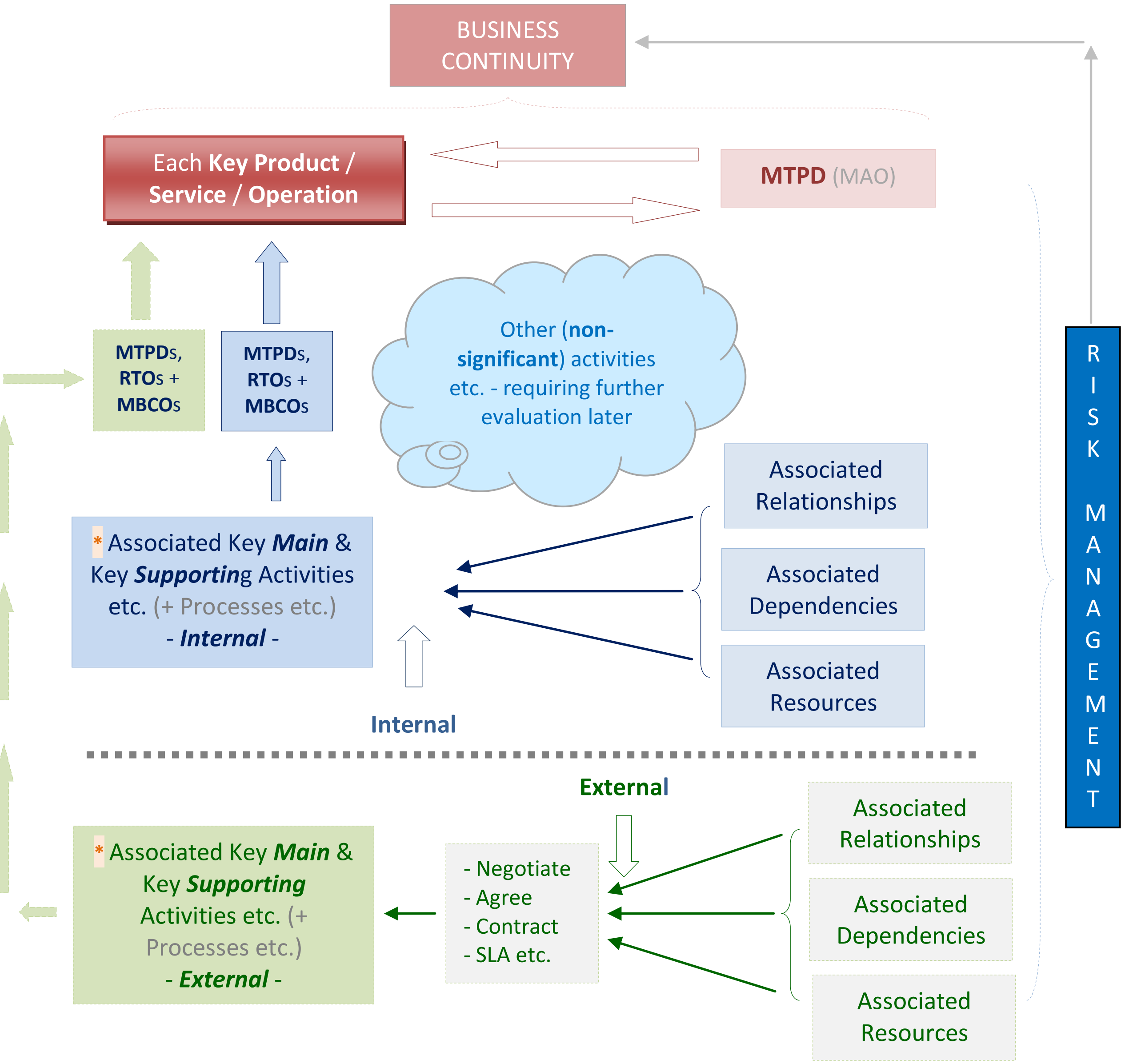
It can also take considerable time and effort to complete - depending on the size and / or complexity of the organisation, the scope of the BIA, the co-operation of participants and resource providers (including budget) - together with the competence / experience / availability of the person(s) undertaking the associated data gathering + analysis of same

Reminder: In ***this*** guideline the ***BIA*** is addressed first before we move on to complete the ***RA***

There is, however, no reason why this sequence cannot be changed. There are advantages and disadvantages to both but, if completed correctly, the end result should be the same for any particular set of given circumstances

Figure **10** - **BIA** - Indicating relationships between:

Key Product / Service / Operation → **Key Activities etc.** → Interdependencies → Resources


BUSINESS CONTINUITY
Each Key Product / Service / Operation
MTPD (MAO)
MTPDs, RTOs + MBCOs
MTPDs, RTOs + MBCOs
Other (non-significant) activities etc. - requiring further evaluation later
* Associated Key Main & Key Supporting Activities etc. (+ Processes etc.) - Internal -
Associated Relationships
Associated Dependencies
Associated Resources
Internal
External
* Associated Key Main & Key Supporting Activities etc. (+ Processes etc.) - External -
- Negotiate
- Agree
- Contract
- SLA etc.
Associated Relationships
Associated Dependencies
Associated Resources
RISK MANAGEMENT

- * = Activities, processes, procedures etc. considered to be '***significant***' as per BIA criteria used
- '***Subordinate***' MTPDs must be equal to or less than their (associated) '***parent***' MTPDs
- All RTO times must fall within their ***associated*** MTPD times
- An RTO ***initially*** selected for a particular activity/process ***may require eventual adjustment*** (but only by shortening) - as a result of an RTO being calculated for a different activity/process - ***in circumstances where some form of interdependency exists*** between said activities/processes
- ***Resources required for BC operations*** are a component part of the overall 'understanding the organisation' process - see 'The (BC Requirements) - Resources Analysis' (Pages 192 & 215)

Business Impact Analysis / *continued*

The BIA (along with the other 3 elements of the 'understanding the organisation' concept [see bullet point list page 123]) is an essential starting point for developing any BCMS project

BIA outputs typically lead on to many important areas associated with managing the ***impacts*** of certain disruptions (should the latter actually occur) e.g. the setting of BC strategy; the formulation (within BC strategy) of BC Tactical Solutions / Treatments etc. (control measures); the identification and production of the associated 'response systems' and plans etc; tentative identification of the appropriate resources required etc.

Get the BIA wrong and the associated BCMS will inadequately / incompletely provide for the organisation's business continuity requirements

As assessing the potential impacts of a significant disruption event on an organisation is typically subjective in nature, the BIA process tries to reduce such subjectivity (to some degree at least) by providing a ***consistent*** set of ***rules*** (methodology) and ***measurement criteria*** - to be applied (to [BCMS] in-scope parts of the organisation) throughout the BIA process

It is essential to obtain informed, objective (i.e. as objective as possible / practicable) and complete input during the BIA. Accordingly, the associated communication and consultation processes with those providing such BIA inputs (subject matter experts etc. - inside and outside of the organisation) are particularly important to manage effectively and efficiently

Business Impact Analysis - **The Process** (Methodology)

1. Top management to approve and appoint an ***appropriately skilled / competent / qualified person(s)*** to ***conduct & manage the BIA*** (use ***external*** resources if necessary)

   Note 1 - It is assumed that the appointed person(s) (e.g. the organisation's 'BC Manager' or a small project team headed by same) will manage / complete / delegate the tasks shown below

   Note 2 - That same person will also typically carry out the other 'understanding the organisation' type tasks

2. Top management to approve (in principle) provision of the estimated ***resources*** (including internal personnel resources, budget etc.) necessary to conduct the BIA (to be confirmed is Step 4 - see next page) (+ also necessary for the ***other*** 'understanding the organisation' type tasks)

3. Complete appropriate ***preparations*** e.g.

   - Establish and document the ***scope*** and ***context of the BIA*** and how it is to be ***practically conducted*** (e.g. methodology & supporting BIA procedures). Include details of the planning & co-ordination processes to be used for the associated data gathering and analysis tasks

- Identify, document and establish the BIA ‘criteria’ ***consequence / impact*** categories to be used (review appropriate info - starting page 148)

- Identify, document and establish the BIA ‘criteria’ to be used when ***quantifying*** and / or ***qualifying*** the ***impacts*** and associated ***timescales*** (over which such impacts might be assumed to act) (review appropriate info - starting page 148)

- Prepare & document a reasonable number of appropriate and realistic ***BC / BIA related scenarios*** (the larger / more complex the organisation - the more scenarios required [subject to scope of the BIA] within reason) which can be used to better demonstrate (to those who will be providing the required BIA information inputs) what will be required as per step 8 further below. ‘Worst case’ (but reasonably realistic) scenarios should typically be used

4. Ascertain & document the ***resources required*** (see step 2 further above) and ***by when*** they should be available

5. Identify organisation’s ***key product(s)*** */ services / operations* etc.

   Document and prioritise **EACH** key product / service / operation (*using some form of* * *‘critically **time** sensitive’ [or otherwise* * *‘critical’ e.g.* ***where safety of life is a factor regardless of the time element]*** ***scoring*** *system to assess and assign such* ***priority***)

   * As defined in BIA ‘criteria’ - (review appropriate info - starting page 148)

   The results (scores) should be appropriate to the continued functionality of each such key product / service / operation (under specific consideration) to the organisation - in the event of same being adversely impacted by ‘significant disruption’ for a ‘significant period’ of time)

   ‘Stakeholder / Other Interested Party Analysis’ outputs could assist in the above task

6. Obtain top management’s ***agreement / approval*** .... to / of outcomes re steps 3, 4 and 5 just above

7. ***Obtain*** and / or *facilitate use* of the various (already identified and now approved [as per step 6. Above]) ***resources*** required to conduct the BIA

8. ***Collect, document and analyse the*** *(BIA related)* ***required data***

   Typically conducted by means of any / all of workshops, questionnaires, interviews & similar - targeted specifically at those (subject matter experts etc. within and outside of the organisation) best able, qualified, experienced, knowledgeable etc. - to provide the required information, data, achieve what is necessary etc.

For example and as a general guide:

- ***Interviews*** (one on one or small group concept) can provide ***good quality*** information / data. The interviewer can directly control (to a degree) what is provided (including the level of detail + its relevance and consistency). Interviews are typically time consuming / work intensive

- ***Questionnaires*** can provide large amounts of data quickly - but the reliable return of completed documents can be problematic and the information / data provided can be of ***poor quality***, be inconsistent etc. (e.g. if the associated methodology / progress is not adequately managed / monitored etc.)

- ***Workshops*** provide reasonably rapid results and are also an opportunity for hands-on engagement (by larger numbers of participants than e.g. in 'interviews') with the BCMS, provided there is attendance and consistent buy-in from the appropriate subject matter experts. (There should be of course - as all of this [at least within the organisation itself] should have ***already*** been approved and pushed down the line by top management as '***must do***')

  In general, the relevance, quality and consistency of information / data obtained from workshops should be ***medium*** to ***good***

- Well managed combinations of ***all*** of the above methods can deliver excellent results in a reasonable timeframe i.e. providing an appropriate level of detail and a standard reporting format, which will assist in consistency of recording and analysing the provided information, across multiple functions

9. ***Use analysis results*** to calculate & document an appropriate (estimated) ***MTPD*** for ***each*** identified ***key product*** / *service / operation* etc.

10. Obtain top management's ***approval*** to outcomes of steps 8 & 9 above

11. ***Make further use of analysed data to complete and document*** steps 12 to 22 below:

    Note 1 - a 'process mapping' analysis (see Glossary) might be useful in facilitating the above

    Note 2 - see step 21 further below ***NOW*** i.e. before returning here to carry on with step 12

12. For EACH identified ***key product*** / service / operation (see step 5 above) - now further identify the appropriate, associated (subordinate) ***key main activities***. (NB: All of the latter [both ***internal*** and ***external*** to the organisation] should be accounted for)

    Document and prioritise EACH such key main activity (*using some form of* * *'critically time sensitive'* *[or otherwise* * *'critical' e.g. where safety of life is a factor regardless of the time element]* ***related*** ** ***scoring*** *system to assess and assign such* ***priority*** *placing*)

    * As defined in BIA 'criteria' - (review appropriate info - starting page 148)

** 'Score' each result in 'units' of ***impact assessment*** (for eventual input into the ***risk management*** [assessment] matrix [see examples in figures 12 to 17, pages 156 to 165 {but read notes bottom of page 155 and page 156 first}]) ***AND*** also in terms of '***priority for action** to be taken*' (e.g. 'highest', 'high', 'medium', 'low' and 'for possible future attention')

The results (scores) should be appropriate to the continued functionality of each such key product / service / operation (under specific consideration) to the organisation - in the event of same being adversely impacted by 'significant disruption' for a 'significant period' of time

'Stakeholder / Other Interested Party Analysis' outputs could assist in the above task?

13. For ***each*** key main * activity identified in step 12 above (and in the scored '***priority for action'*** order - as appropriate) - estimate and document an appropriate ***MTPD*** and (associated) *initial* ***RTO*** - such that the latter MTPD estimations are ** compatible (i.e. equal to or shorter) with the (separate) ***MTPD*** estimations of the associated (parent) key product / service / operation (latter as per step 9 further above)

    Where (if) any of such MTPDs and RTOs relate to ***external*** organisations - estimation and application of same will need to be mutually negotiated and agreed accordingly - e.g. via contractual 'service level agreements (SLA)' or similar

    * Reminder - from the glossary meaning of the term '**activity**' as used herein, most (if not all) ***activities*** typically comprise a series of associated ***processes*** (which in turn typically comprise a series of associated ***procedures*** etc.). For the sake of simplicity and brevity the latter (processes & procedures) have been generally ignored in this Section 5 / 2B

    However, when conducting a BIA **in reality**, all such processes & procedures (as associated with key ***main*** activities as per this step 13.) **must** ***additionally*** be accounted for of course - and any considered 'significant' (as per BIA criteria) should be assigned MTPDs, initial RTOs and initial MBCOs ***in their own right*** - and managed accordingly as per the above and below info

    ** Note - where a key main activity ***MTPD*** estimated as per above is ***longer*** (in terms of time duration) than the ***MTPD*** for its associated (parent) key product / service operation - then the situation **must** be reviewed and the required 'compatibility' attained e.g. by lengthening the MTPD for the parent key product etc. (if acceptable); by shortening the MTPD for the subordinate key main activity (if acceptable / possible); or by a mix of both

14. For **EACH** identified key main activity (as per step 12 above) - identify and document the appropriate, associated (subordinate) ***key supporting activities***. (All key supporting activities [i.e. both internal and external to the organisation] to be accounted for)

    Document and prioritise **EACH** associated key supporting activity (*using some form of * 'critically time sensitive' [or otherwise * 'critical' e.g. where safety of life is a factor regardless of the time element] related ** **scoring** system to assess and assign such* ***priority***)

    * As defined in BIA 'criteria' - (review appropriate info - starting page 148)

** 'Score' each result in 'units' of ***impact assessment*** (for eventual input into the ***risk management*** [assessment] matrix [see examples in figures 12 to 17, pages 156 to 165 {but read notes bottom of page 155 and page 156 first}]) ***AND*** also in terms of '***priority for action***' to be taken (e.g. 'highest', 'high', 'medium', 'low' and 'for possible future attention')

The results (scores) should be appropriate to the continued functionality of each such key supporting activity (under specific consideration) to the organisation - in the event of same being adversely impacted by 'significant disruption' for a 'significant period' of time

'Stakeholder / Other Interested Party Analysis' outputs *might* assist in the above task?

15. For ***each*** key supporting * activity identified in step 14. above(and in the scored '***priority for action***' order - as appropriate) - estimate and document an appropriate ***MTPD*** and (associated) *initial* ***RTO*** - such that the latter MTPD estimations are ** compatible (i.e. equal to or shorter) with the (separate) ***MTPD*** of the associated *(parent)* key main activity (latter as estimated in step 13 further above)

Where (if) any of such MTPDs and RTOs relate to ***external*** organisations - estimation and application of same will need to be negotiated and agreed with any such organisation e.g. via contractual 'service level agreements (SLA)' or similar

* Reminder - from the glossary meaning of the term '**activity**' as used herein, most (if not all) ***activities*** typically comprise a series of associated ***processes*** (which in turn typically comprise a series of associated ***procedures*** etc.). For the sake of simplicity and brevity the latter (processes & procedures) have been generally ignored in this Section 5 / 2B

However, when conducting a BIA ***in reality***, all such processes & procedures (as associated with key ***supporting*** activities as per this step 15.) must ***additionally*** be accounted for - and any which are considered 'significant' (as per BIA criteria) are to be assigned MTPDs, initial RTOs and initial MBCOs ***in their own right*** - and managed accordingly as per the above and below

** Note - where a key supporting activity ***MTPD*** estimated as per above is ***longer*** (in terms of time duration) than the ***MTPD*** for its associated (parent) key main activity - then the situation must be reviewed and the required compatibility attained e.g. by lengthening the MTPD for the parent key main activity etc. (if acceptable); by shortening the MTPD for the subordinate key supporting activity (if acceptable / possible); or by a mix of both

16. For all internal and external key main activities & key supporting activities (and thus their associated processes, procedures etc. also) addressed in steps 12 to 15 above - identify ***all associated and appropriate dependent / inter-dependent*** matters, subjects, relationships etc. Document *each such dependency / inter-dependency etc.* assessed as having a * significant influence on each such activity / process (specifically the possible requirement for 'knock-on effect' adjustments to be made to existing [initial] RTOs - which may ***not yet*** have been accounted for)

* As defined in BIA 'criteria' - (review appropriate info - starting page 148)

17. Analyse the results of step 16. Where so required *adjust all **initial** RTOs* from steps 13 & 15 above, accordingly

    For example - if activity A depends for its recovery upon activity B, then the RTO of activity B must be ***equal to or less*** than the RTO of activity A

    That is, if the ***originally calculated*** RTO for activity B was greater (***longer***) than the RTO for activity A - then activity B's original RTO must now be shortened accordingly such that it is equal to or less than activity A's RTO

    If the latter is not possible (for whatever reason) then activity A's RTO must be lengthened so as to be the same as activity B's RTO

    Where ***initial*** RTOS are so adjusted a check of all associated MTPDs must then be made and, where necessary, adjusted in turn (to accord with the MTPD related requirements of items 13 & 15 above)

18. Decide, assign and document the ***MBCOs*** to be achieved when disrupted activities are assumed / planned to 'resume' at the associated RTOs

19. Identify and document *'**single points of failure**'*

20. Use ***impact*** level assessments (scores) from steps 12 and 14 above *as **inputs*** to the risk management (assessment) process (see page 167)

21. Whilst conducting steps 12 to 17 further above - also identify and document those internal and external activities (+ their associated processes, procedures etc.) if any, which, whilst not having been allocated a significant priority (score) level in this formal part of the BIA, ***are still thought** (for some valid reason) **worthy of inclusion*** from a BC context. This list will eventually be reviewed to see if any such activity / process etc. is worthy of re-consideration for inclusion in the BC strategy / tactical solution process *OR* for inclusion in some form of minor (informal) continuity programme *OR* can be ignored

22. Pull together & document the results of all of the above into a report which, (when combined with the results of the ***other three components*** [business tools] of the 'understanding the organisation' process [see page 123]and approved by top management) will be used in due course to formulate an associated * **'BC Strategy'**

    * It will be recalled that ***BC Strategy***, in turn, outlines [from the higher level viewpoint] what the organisation needs to achieve going forward from (after) the BIA has been completed, for example (list is far from exhaustive)……………………:

- Formulation of '**BC** (Tactical) **Solutions** / Treatments / Controls etc.'
- Setting up of the '**Incident Response Structure**'
- Production of the associated **BC Plans** etc.

Reminder of Key Definitions

- **Maximum Tolerable Period** of **Disruption** (MTPD) (Maximum Acceptable Outage - **MAO**)

  Estimated period of ***time*** it would take for the consequences of an adverse impact(s), arising as a result (for whatever reason - but typically termed 'disruption / interruption') of **not** providing an organisation's **key** product(s) / service(s) / operation(s) / activities etc. (for whatever reason) - **to become unacceptable** to the organisation's (impacted) stakeholders / other interested parties

- **Minimum Business Continuity Objective**(s) (MBCO)

  Pre-planned ***minimum*** / ***acceptable etc. delivery levels*** of an organisation's key product / services / operations etc. - together with (**+**) the latters' associated, subordinate activities etc. (all as related to various [potential] ***disruption*** scenarios) - ***predicted*** as being ***achievable*** by a ***pre-defined*** Recovery Time Objective(s) (RTO)

  Note - '***pre-planned delivery levels***' etc. (as per definition above) are typically stated in terms of 'time-prioritisation e.g. '…………….an MBCO of 25 % to be available **within *two* hours**; 50 per cent **within *two* days**; full (normal) service **within *one* week** etc………….'

- **Recovery Time Objective** (RTO) - (RTO concept is typically that of a '***prioritised timeframe***')

  A pre-determined target ***time*** set by an organisation for * resuming *key* **main** *activities* (and, consequently, the latters' [associated / subordinate] *key* **supporting** *activities* - where appropriate) to a pre-determined level of output (see MBCO) - following an associated, disruption type event

  (Reminder: In ascending order - *key* **supporting** *activities* relate to their associated [parent] *key* **main** *activities* - which relate in turn to their associated [parent] *key* **product**(s) / **service(s)** / **operation(s)** / **activities** etc.)

  Set RTO too late & the organisation could encounter big resumption problems. Set it too early & the associated costs of managing same might outweigh the benefits

  * The terms '***resuming***; ***resumption***' etc. should not necessarily be taken as being related to ***normal*** *(full)* delivery levels of a product, service or operation etc. - although the latter would still be the case in certain circumstances e.g. for a surgical operating theatre; for some emergency services & similar etc.

Notes regarding 'BIA' Steps 1 to 22 above (in no particular order)

Training (Familiarisation)

Further to step 8 further above, it would be beneficial to provide some relatively brief and low-key training for * those persons assigned to provide the information required. Such training, when combined with provision of a good quality methodology document (written instructions on how to provide what is required) can be of significant overall benefit to the BIA process - and so is well worth doing

* Specifically those persons (within and outside the organisation [e.g. suppliers for the latter]) most qualified and experienced etc. so to do (e.g. subject matter experts). In general, the BC Manager, external consultants etc. are ***not*** able to provide what is required here

'Owners' of Key Main Activities / Key Supporting Activities / Processes etc. / Dependencies

Re steps 12, 14 & 16 further above, also identify and document the 'owners' (persons directly responsible / accountable) of the activities, processes, procedures, dependencies etc. involved. If the owner is not also the subject matter expert, ensure that both are involved (contribute) in (to) the appropriate part(s) of the data gathering process

Making Money

For commercial (profit making) organisations it is particularly important that an organisation's revenue earning activities (departments / business units etc.) provide appropriate inputs to the BIA - particularly regarding what level of (disruption related) impact might be 'acceptable' to specific revenue generating activities. They will also be able to provide advice to the BC Manager on the formulation of appropriate (financial related) '***consequence / impact categories***'(see figure 11 / page 157)

Step 16 - Dependencies and Interdependencies

identify the dependencies of the various components of key activities, processes etc. (including people, information and data, facilities [buildings, workplaces and associated utilities], equipment, consumables, ICT systems, transportation, logistics, finance, partners, supply chain etc.). As an example, the primary dependency for the vast majority of airlines, airports, GHAs etc. to account for, is likely to be the availability of ICT (systems, software, hardware etc.) + its associated power sources (mains electricity, UPS, generators etc.) + its maintenance etc.

Also identify any associated interdependencies e.g. procurement ops are dependent on finance assigning and releasing the associated funds

Calculation of RTOs

In *this* guideline the calculation of RTOs & MBCOs is made here in Section 5 / 2 - as part of the 'understanding the organisation' task i.e. resulting from the BIA. Other 'schools of thought' assign RTOs etc. in the 'Setting BC Strategy' task which follows on at a later point in the BCMS process. From practical / logical / common sense viewpoints, however, RTO assignment during the BIA ***does*** have its advantages and is the method adopted herein

BIA - Outcomes

Regarding the involved organisation, the outcomes from a BIA should typically provide:

- A list of 'in-scope' key products / services / operations (typically prioritised in terms of disruption impact on [associated] significant factors identified by the organisation - including direct / indirect revenue)
- A list of key *main* activities & component processes, procedures etc. (internal and external & *similarly prioritised as per top bullet point above*) - which contribute to the delivery of the related key products / services / operations
- A list of key *supporting* activities + component processes, procedures etc. (internal and external & *similarly prioritised as per top bullet point above*) - which contribute to the delivery of the related key main activities
- Estimation of MTPDs (with justification[s])
- *Initial* estimation of RTOs (with justification[s])
- A list of dependencies / interdependencies
- *Final* estimation of RTOs (with justification[s]) - after adjustment of initial estimates (where required) due 'knock-on' effects of e.g. dependent / inter-dependent activities
- Estimation of MBCOs (with justification[s])
- A 'single points of failure' list
- A list of selected activities which did not 'quite' meet the BIA's 'significant' level criteria (will be used for another 'look at' at some [not too distant] future point)
- Derived 'impact levels' for input to the associated risk assessment procedure
- Completed documentation re all of the above
- Top management review and approval of the BIA
- Inputs for the BC Strategy (including initial Identification of supporting resources going forward in this BCMS implementation (**DO**) phase [see 'BC - Resources Requirements Analysis' - page 135])

Reminder - for simplicity, only MTPD & RTO have been considered in this guideline document. However, when planning BC strategy for resumption & recovery of ***information / data*** and similar issues in reality, ***MTDL*** & ***RPO*** will also apply (see Glossary)

BIA - Methodology and Choosing Appropriate Criteria

Step 1

Identify Organisation's** (Strategic) **Business Objectives

Undertake research to understand the strategic objectives (i.e. ***not*** the BC objectives) of the organisation's business - the latter being its high level (strategic / big picture view) planned objectives - sometimes termed 'business aims, objectives, drivers, vision, mission etc.'…………… i.e. those factors which contribute to the basic fulfilment of the purpose of the organisation

Note - one would expect the organisation's strategic objectives to already be formally defined and documented 'somewhere' - but this may not always be the case!

If the strategic objectives *are* already defined - then use them directly. However, it is worth at least reviewing them before commencing a BIA - to ensure that they reflect 'reality'. If the strategic objectives are ***not*** yet defined (or are inadequately defined) - fix up (with TM approval) workshop(s) with senior execs from organisation's key areas, in order to complete this step 1

Appropriate representatives from all levels of the organisation should also be either involved or consulted where felt appropriate - together with input from external representatives such as key suppliers, parent organisation etc.

When complete, confirm and obtain agreement & approval from top management on said strategic objectives of the organisation. (Such objectives should be concisely defined, measurable and accountability allocated for each. They should be documented)

Step 2

Methodology

Already covered further above (pages 141 - 147)

Step 3

Choosing Appropriate Criteria

Decide upon and gain approval for the quantitative and qualitative BIA ***criteria*** (i.e. the '*units*' to be used to ***measure*** and ***assess*** respectively the levels of ***impact*** caused by uncontrolled / non-specific disruption) specifically appropriate to the organisation. The criteria should be aligned as closely as possible with the organisations ***strategic*** *business objectives* (see step 1 a little further above). Examples of such criteria might include (the list is not exhaustive):

Example: Criteria

Consequence / Impact *Categories* - ***General***

Note: The term '***consequence*** / ***impact categories***' refers to those key main and key supporting activities and their inter-dependencies (being directly and / or indirectly associated with delivery of an organisation's *key product / services / operations*) - which, if disrupted (typically adversely) in some way as a result of a realised risk (threat) occurrence, ***might*** consequentially have a significant, adverse ***impact***(s) on the ability of the organisation to deliver said key product / services / operations

Consequence / Impact Categories must be specific to the organisation ***and*** activity they apply to

Examples of some generic consequence / impact categories include……….financial; operational effectiveness / efficiency; brand / image / reputation type issues; stakeholders (particularly customers / clients and shareholders); statutory / regulatory; injury / death etc. For aviation in particular we can add e.g. the categories of 'aviation safety' and 'aviation security'

To ensure consistency within an (the same) organisation with regard to the closely associated subjects of risk management (assessment) and business (continuity) impact assessment, a ***common or near common set of consequence*** / ***impact categories*** should be available and applied to ***both*** processes

When conducting the information gathering task for the BIA, the below *'**categories**'* might be considered as the basis for questions regarding the *'**consequences / impacts**'* of disruption to 'activities' within (and without as applicable) the organisation, if same are not resumed (at least to a certain, defined recovery level e.g. this will lead eventually to decisions regarding MBCO) within defined timescales (e.g. this will lead eventually to decisions regarding MTPD and RTO). The below list is ***not*** exhaustive (i.e. it is representative only)

- Consequences / Impacts - **Customers / Clients**
  - How quickly might customers become aware of the 'problem'
  - How might they react (e.g. severe customer dissatisfaction)
  - What is the likelihood that they will take their business elsewhere
  - What might be the impact upon pre-agreed levels of service to be provided
  - What might be the impact upon customer supply chain(s)
  - What physical / mental harm might be caused to customers

- Consequences / Impacts - **Financial Considerations** (Phrase the below 'criteria' as questions e.g. 'when might………………….'; 'how might; 'what will………………….' etc.)
  - Loss of revenue (e.g. revenue losses exceeding $ USD xxxxx per day)
  - Additional costs associated with resumption & recovery
  - Overtime payments
  - Travel costs and expenses
  - Increased Insurance costs
  - Replacing lost equipment, raw material and supplies
  - Loss of raw materials / finished products
  - Clean up and restoration costs
  - Impact on cash flow
  - Impact on market share
  - Impact on future sales
  - Impact on stock market share price
  - Contractual fines and / or penalties
  - Lawsuits etc.
  - Loss of financial control
  - Bankruptcy
  - Cessation or limitation of operation

- Consequences / Impacts - **Legal / Regulatory Considerations** (Phrase the below 'criteria' as questions e.g. 'when might………………….'; 'how might; 'what will………………….' etc.)
  - Reduction / loss of safety margins
  - Fines
  - Financial penalties (e.g. penalties exceeding $ USD yyyyy per day [quantitative])
  - Criminal / Civil Law penalties (including imprisonment)
  - Cessation or limitation of operation

- Consequences / Impacts - **Operational Considerations** (Phrase the below ‘criteria’ as questions e.g. ‘when might…………………’; ‘how might; ‘what will…………………’ etc.)
    - Reduced service and / or quality levels
    - Reduced operational levels (e.g. operational safety compromised)
    - Overtime requirements
    - Workflow disruptions
    - Supply chain disruption
    - Backlog clearance
    - Seasonal variations
    - Inability to meet deadlines
    - Loss of operational control
    - Cessation or limitation of operation

- Consequences / Impacts - **Reputation / Brand / Image Considerations** (Phrase the below ‘criteria’ as questions e.g. ‘when might…………………’; ‘how might…………………’; ‘what will…………………’ etc.)
    - Media attention (e.g. serious [adverse] publicity in all forms and types)
    - Environment attention (e.g. causing serious damage to the environment)
    - Shareholder confidence (e.g. vote of no confidence in ‘board of directors’; e.g. corporate governance requirements seriously breached / not upheld)
    - Competitors taking advantage of situation
    - Cessation or limitation of operation

- Consequences / Impacts - **People / Humanitarian Considerations** (Phrase the below ‘criteria’ as questions e.g. ‘when might…………………’; ‘how might; ‘what will…………………’ etc.)
    - Death and / or injury to customers / clients
    - Loss of staff (e.g. inability to get to work; death, illness or injury, strike [industrial action] etc.)
    - Unemployment
    - Community issues
    - Shorter and longer term mental trauma
    - Provision of humanitarian assistance and welfare
    - Knock-on effects to staff and their families
    - Compensation
    - Cessation or limitation of operation

- Consequences / Impacts - **Environmental** (Phrase the below ‘criteria’ as questions e.g. ‘when might…………………’; ‘how might; ‘what will…………………’ etc.)
    - Pollution
    - Human health considerations
    - Environmental health considerations etc.

Reminder - do not confuse ‘***risk***’ with ‘***consequences*** / ***impacts***’ e.g. ‘injuries’, ‘financial loss’ and ‘reputation damage’ etc. - are **not** risks……………………they are ***consequences*** of realised risk

Example: Criteria

*Consequence / Impact Categories - Expressed **Qualitatively** and / or **Quantitatively***

Consequence / Impact categories may be expressed qualitatively, quantitatively or as a mixture of both. ***Very*** generally speaking, qualitative type terminology ***might*** be more appropriate to smaller / simpler organisations, whilst a mix of qualitative and quantitative terminology / units ***might*** better suit the larger / more complex organisation

Furthermore, (e.g.) 'financial type impacts' are typically (but not always) expressed quantitatively - whereas 'brand / image / reputation' type impacts may be expressed qualitatively or by a qualitative / quantitative combination

Note: - ***financial quantifications*** re appropriate activities are perhaps one of the hardest aspects of the BIA to adequately assess, as revenue generation is typically not a constant / linear flow but is instead usually somewhat irregular e.g. look at the difference between an airline's revenue in low season vs peak season. Consequently, the financial costs of disruption can vary significantly

One solution might be to consider the problem from the financial target or budget perspective i.e. each such activity will typically have an effective daily or monthly target derived from the annual financial targets. Part of the income might be e.g. from ongoing revenue streams, with the balance coming from new business. It is the latter which would be hit hardest during a significant disruption event

Another approach might be to build up the projected financial losses over time as some activities may not have an immediate impact - but one which might start e.g. a week or two later. Additionally there may be financial losses from non-revenue generating areas of the organisation e.g. regulators may impose fines or certain interested parties may make breach of contract claims. All should be recorded, combined and considered to try to give an idea of what the worst case financial impact(s) might be

For more detailed information on qualitative and quantitative impact categories see (separate document in this series) CRPM Part **3** / Volume **1** - Appendix **C**

Example: Criteria

*Consequence / Impact Categories - The '**Time**' Factor*

Disruption planning and the application of associated BC countermeasures (BC Tactical Solutions / Treatments / Controls etc.) are typically linked by ***time*** e.g.

- ***When*** will the effects of a disruption start to impact adversely on an organisation's key activities etc?
- ***When*** does this impact become significantly adverse enough to become unacceptable? And consequently……………..
- ***When*** does the organisation need to activate the associated BC countermeasures etc?

The time taken for impacts to become unacceptable may vary from seconds (e.g. unexpected and total cessation of a busy airport's air traffic services - for whatever reason) to several months or more (e.g. gradually reducing customer numbers - again, for whatever reason)

Excepting for immediate / near immediate type unacceptable impact consequence situations, the point at which an adverse disruption becomes unacceptable (if at all) is usually (simplistically speaking) a gradual process with regards to the time when the disruption first commenced (see pages 157 to 165 for examples [but read notes bottom of page 155 and page 156 first])

Such 'unacceptability' regarding time-sensitive activities might need to be specified e.g. to the minute, to the hour etc. Less exacting accuracy will be acceptable for less time-sensitive processes e.g. days, weeks, months or even longer - the rebuilding of a destroyed office facility being an example of the latter. And to re-iterate, some activities, regarded as 'mega' critical, do not pedantically have a time-sensitive limit for resumption, other than 'immediate' - again, using here the example of an emergency 'surgical operating theatre'

Example: Criteria

(Degree / Level / Amount etc. of) ***Impact***

The 'measurement' of (disruptive) ***impact*** in smaller / simpler organisations might typically be termed * 'High, Medium or Low'. For larger / more complex organisation a rating of 1 to 5 (or 'A' to 'E' if preferred) is typically used - '1' or 'A' being least impacting and the opposite for '5 or 'E'' - the latter usually being rated / scored as e.g. 'catastrophic / near catastrophic' or equivalent term

* **Note** - let's 'put some meat on the bones' regarding what is typically meant above when using the terms 'high, medium and low' and / or their numerical equivalents and similar - with regards to **impact levels**:

High Impact (H) = The department / business unit in question **1)** cannot operate without this particular activity / process / resource for even a relatively short period of time AND / OR **2)** may experience a very high recovery cost AND / OR **3)** may realise very serious problems in achieving the mission and / or in maintaining reputation AND / OR **4)** may experience human death or serious injury etc.

Medium Impact (M) = The department / business unit **1) could** work around the loss of this particular activity / process / resource e.g. for a few days or perhaps a week, but eventually restoration must occur AND / OR **2)** may experience significant cost in recovery AND / OR **3)** may realise significant problems in achieving the mission and / or in maintaining reputation AND / OR **4)** may experience significant human injury etc.

Low Impact (L) = The department / business unit **1)** could operate without this this particular activity / process / resource for an extended (but not indefinite) period of time during which particular units or individuals may be inconvenienced and / or need to identify alternatives, or **2)** may notice a degree of adverse effect on achieving the mission and / or maintaining reputation

Reminder - The BIA derived ***impact*** 'measurement / assessment' of a disruption event upon a specified activity / process etc. - provides one input into the ***risk management*** *(assessment)* ***matrix***. The other input (***probability / likelihood*** of a specified threat actually occurring [being realised] to a specified activity) - comes from the ***risk assessment*** process directly

Example: Criteria

Priority

Activities which are subject to a significant (adverse) impact (as a result of an associated disruption event) are assigned a 'priority' which dictates the order in which they need to be 'dealt with' - from the BC viewpoint

Again, the criteria can be set in plain language (highest / high / medium / low / lowest) and / or by use of an alpha-numeric equivalent e.g. 1A, 1B etc. for highest priorities; 2A, 2B for high priorities - and so on. Note that in this latter system '1A' would have a higher priority than '1B' - even though both fall within the 'highest' priority category overall

*Criteria - **IMPORTANT NOTE***

It will be noted from the above that measurement criteria are used in several different parts of the **BIA** (with a further '*measurement*' [i.e. likelihood / probability] coming from the ***RISK MANAGEMENT*** [assessment] process - as will be seen a little later in this guideline)

To avoid confusion, common sense and logical use of appropriate combinations of 'plain language' and / or 'alpha-numeric' criteria should be applied with care

Also take careful note that **BIA** related activity '***Impact*** (Level / Amount etc.) Criteria' is a totally different subject / parameter to **BIA** related activity '***Priority*** Criteria' - don't get confused between the two (although the two are likely to be closely linked)

Note: Alpha-numeric criteria are also typically used in the 'pure' ***risk assessment*** process (see pages 180 - 186) i.e. ***not*** involving BC. This is another potential cause of 'confusion' ***unless*** the various contexts in which such criteria are used, are clearly understood and applied

*Criteria - **Examples***

Some examples of how 'criteria' might be applied during a BIA are shown on pages 157 to 165

Notes:

- All criteria, MTPDs / RTOs / MBCOs etc. used in figures 11 to 17 are provided for example purposes only. Whilst some thought has gone into them in order to hopefully achieve an appropriate degree of realism - ***they remain 'fictional' of course***. Please always keep this in mind when studying them

*(The **actual** / **real** information required will, of course, come from consultation with the organisation's appropriate subject matter experts - during the BIA procedure itself)*

- Figure 11 is a ***generic*** example only (e.g. it is ***not*** aviation specific). In reality, it will be necessary to derive consequence / impact categories specific to the type of aviation business under consideration e.g. for a specific airline; for a specific airport; for a specific GHA etc.

- Figures 12 to 17 ***are*** aviation related examples

- Figure 12A - the BIA '**priority**' for dealing with this ***particular*** risk had been set (purely for example purposes - but in this case it is probably fairly realistic) at the highest possible level - represented (**priority** criteria) by the number '1'. However, ***other*** activities within 'ABCX Airways' will also fall into this top priority - as is the case in the example shown in figure 13

  To differentiate between them (e.g. looking at all activities assessed as 'priority 1') we have accordingly used a 'refinement' of the ***priority criteria*** by adding capital letters after the number e.g. '1A'; '1B' etc. - with 1A taking priority over 1B…………and so on. This refinement has been adopted in the examples shown in figures 12 to 17 e.g. the 'priority 1' originally assigned in figure 12 is now changed to 'priority 1B' - due a higher priority activity (i.e. priority 1A) having been identified in figure 13

- Whilst figure 12A is an example suitable to a larger / more complex airline, figure 12B portrays the same thing (same activity, risk etc.) - but now in a simplified format as might be better related to the smaller / less complex operator

- For convenience, figures 14 to 17 have also been shown in the 'simplified' version. However, where the size and / or complexity of the organisation so requires, the full version (as per figures 12A and 13) should be used

- Please now see the 'important' notes on page 165 ***before*** reading further

VERY IMPORTANT NOTE

It was decided to place figures 11 to 17 on the following [specific] pages as ***some*** of the info provided (e.g. Consequence / Impact Categories; Degree / Level / Amount of Impact; Priority for Action etc.) relates directly to what you have just been reading under the BIA element of 'understanding the organisation'

However, figures 11 to 17 also include info re the associated risk assessment (RA) process (see Section 5 / **2B** / **3** starts page 167) - also being part of 'understanding the organisation'

Accordingly, it is suggested that the risk assessment section (referred to just above) is ***also*** studied - ***BEFORE*** looking at figures 11 to 17

Also known as ‘***Impact Category***’

EXAMPLE ONLY - Fig **11**

Generic *BIA Reference Matrix* - used to formulate ***impact criteria*** (which in turn are used to provide ***impact assessment*** ‘scores’ for specified activities - see Fig 12)

***CONSEQUENCE** Category* →	**Interruption**	**Op. Efficiency**	**Regulatory etc.**	**Financial**	**Reputational**	**Stakeholder**	**Injuries etc.**	**Other**
***IMPACT** Criteria* ↓	**IMPACT ASSESSMENTS**							
1. Negligible	< 2 hours	Minimal	Minimal	< .025% of op. budget	Minimal	Minimal	None	*TBA*
2. Moderate	2 - 12 hours	Slight reduction	Temporary (minor) non-compliances	.025 to .2% of op. budget	Low ‘news’ value	Some minor impacts	First Aid required	*TBA*
3. Significant	12 - 24 hours	Considerable reduction	Significant non-compliances in the shorter term	.2 to 2% of op. budget	Some damage - moderate news value	Significant impacts to some and / or minor impacts to all	Hospitalisation required	*TBA*
4.Serious / High / Major	24 hours to 1 week	Some key activities not deliverable	Significant to major non-compliances in the medium term	2 to 5% of operating budget	Major damage - high news value - stakeholders ‘taking action’	Major impacts to some and / or significant impacts to all	Some critical injuries and / or deaths	*TBA*
5.Catastrophic	> 1 week	Key products / services etc. not deliverable	Major non-compliances in the longer term / indefinitely	> 5% of operating budget	On-going viability of business threatened	Major and long term impacts to all	Mass critical injuries and / or deaths	*TBA*

The purpose of the above matrix is to provide a ‘common language’ on how impacts (on activities etc.) are evaluated and measured (the latter must be specific to what the organisation ‘does’ of course e.g. banking criteria will be different in some (but not all) areas to that used for airline operations). Note that this matrix is a ***generic*** example and is ***not*** targeted specifically at aviation related key activities etc.

EXAMPLE ONLY - AIRLINE OPERATIONS CONTROL CENTRE (OCC) - ***Comprehensive*** Version - Fig **12A**

BIA Template - Key Activities - ***Comprehensive*** *Version of* **Activity Impact Matrix** (Assuming airline operates 24H on a worldwide basis)

Activity & BIA Assigned Priority: Airline (ABCX Airways) ***OPERATIONS CONTROL CENTRE*** - OCC - **HIGHEST** Priority (e.g. 'Priority 1B')

Risk: ***Complete loss of OCC facility*** (e.g. due fire [the 'threat' in this example]. This '*risk*' would have been derived from a (separate) *RA*

Impact ***Categories*** by 'type'

Impact Categories ↓ ***Impact Durations*** →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
Assess impact on ***passengers*** ops	2	2.5	3.5	4	4.25
Assess impact on ***cargo*** ops	2	2.5	3	3.5	4
Assess ***commercial*** impact	2	2	2.5	3	3.5
Assess ***financial*** impact	2	2	2.5	3.5	4
Assess ***reputational*** impact	1	2	2	2.5	3.5
Assess ***backlog*** (work catch-up) impact	2	2.5	3	4	4.25
Assess impact on ***OCC staff***	2	2.5	3	3.5	4
Assess impact on ***operating crew***	2	2	2.5	3	3
Assess ***legal / regulatory*** impact	2	2	2.5	3.5	4.25
Assess (anything else as appropriate)	*TBA*	*TBA*	*TBA*	*TBA*	*TBA*
Overall Impact Assessment of activity loss	***2***	***2.5***	***3***	***3.5***	***4***

Impact ***Assessments*** - graded ('scored') by degree ('weighting') of ***adverse*** impact criteria

Adverse Impact Criteria (Weightings): 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD*** / ***MAO*** = **24 hours**

Calculated ***Initial RTO*** = **12 hours** *(Note may require 'adjustment' after accounting for 'knock-on' effects of associated interdependencies [if any?])*

MBCO = **50% recovery within 12 hours; 75% within 18 hours; 100% within 24 hours**

Maximum anticipated (adverse) impact assessment beyond ***30 to 36 hours*** outage = **5**

EXAMPLE ONLY - AIRLINE OCC - ***Simplified*** Version - Fig **12B**

BIA Template - Key Activities - ***Simplified Version of*** **Activity Impact Matrix** (Assuming airline operates 24H on a worldwide basis)

Activity & BIA Assigned Priority: Airline (ABCX Airways) ***OPERATIONS CONTROL CENTRE*** - OCC - **HIGHEST** Priority (e.g. 'Priority 1B')

Risk: ***Complete loss of OCC facility*** (e.g. due fire [the 'threat' in this example]. This '*risk*' would have been derived from a (separate) *RA*

Impact Durations →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
	↓	↓	↓	↓	↓
Overall Impact Assessment of activity loss	***2***	***2.5***	***3***	***3.5***	***4***

Adverse Impact Criteria: 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD*** / ***MAO***	= **24 hours**
Calculated ***Initial RTO***	= **12 hours** *(Note may require 'adjustment' after accounting for 'knock-on' effects of associated interdependencies [if any?])*
MBCO	= **50% recovery within 12 hours;** **75% within 18 hours;** **100% within 24 hours**

Maximum anticipated (adverse) impact assessment beyond ***30 to 36 hours*** outage = **5**

EXAMPLE ONLY - Airline (CCC) - Fig **13**

BIA Template - Key Activities - ***Comprehensive*** *Version of* **Activity Impact Matrix** (Assuming airline operates 24H on a worldwide basis)

Activity & BIA Assigned Priority: Airline (ABCX Airways) ***CUSTOMER CALL / CONTACT / INFO CENTRE*** - CCC - **HIGHEST** Priority (e.g. ‘Priority 1A’)

Risk: ***Complete loss of CCC facility*** (e.g. due credible bomb ‘threat’). This ‘*risk*’ would have been derived from a (separate) *RA*

Impact Categories ↓ ***Impact Durations*** →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
Assess impact on ***customers***	2.5	3	4	4.25	5
Assess ***commercial*** impact	2.5	3	3.5	4	5
Assess ***financial*** impact	2	2.5	3	3.5	4.5
Assess ***reputational*** impact	2	2.5	3	4	5
Assess ***backlog*** (work catch-up) impact	2	3	3.5	4.25	4.5
Assess impact on ***call centre staff***	2	2.5	3	4	4.5
Assess impact on ***shareholders***	2	2.5	3	3.5	4.5
Assess (anything else as appropriate)	*TBA*	*TBA*	*TBA*	*TBA*	*TBA*
Overall Impact Assessment of activity loss	***2***	***2.75***	***3.5***	***4***	***4.75***

Adverse Impact Criteria: 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD / MAO***	= **18 hours**
Calculated ***Initial RTO***	= **6 hours** *(Note may require ‘adjustment’ after accounting for ‘knock-on’ effects of associated interdependencies [if any?])*
MBCO	= **50% recovery within 6 hours; 75% within 12 hours; 100% within 18 hours**

Maximum anticipated (adverse) impact assessment beyond ***24 to 30 hours*** outage = **5**

EXAMPLE ONLY - Airline - In-flight Catering Supply (IFC) - Fig **14**

BIA Template - Key Activities - ***Simplified*** *Version of* **Activity Impact Matrix** (Assuming airline operates 24H on a worldwide basis)

Activity & BIA Assigned Priority: Airline (ABCX Airways) ***IN-FLIGHT CATERING SUPPLY*** - IFC - **MEDIUM** Priority (e.g. 'Priority 2A or 2B or 2C' etc.)

Risk: ***Complete loss of IFC Supply*** (e.g. due 'staff industrial action' e.g. due 'food contamination' etc.). This '*risk*' would have been derived from a (separate) *RA*

Impact Durations →	6-24 hrs	24-48 hrs	2 to 4 days	4 to 7 days	7 days +
	↓	↓	↓	↓	↓
Overall Impact Assessment of activity loss	***2***	***2.5***	***3***	***3.5***	***4***

Adverse Impact Criteria: 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD / MAO*** = **5 days**

Calculated ***Initial RTO*** = **3 days** *(Note may require 'adjustment' after accounting for 'knock-on' effects of associated interdependencies [if any?])*

MBCO = **50% recovery within 3 days;** **75% within 4 days;** **100% within 5 days**

Maximum anticipated (adverse) impact assessment beyond 5 to 7 days outage = **4**

EXAMPLE ONLY - Airport - Air Traffic Services (ATS) - Fig **15**

BIA Template - Key Activities - ***Simplified*** *Version of* **Activity Impact Matrix** (Assuming airport operates 24H)

Activity & BIA Assigned Priority: Airport (XYZ Int'l Airport) ***AIR TRAFFIC SERVICES*** - ATS - **HIGHEST** Priority (e.g. 'Priority 1A')

Risk: ***Complete loss of ATS facility*** (e.g. due total electrical / power supply failure). This '*risk*' would have been derived from a (separate) *RA*

Impact Durations →	None Acceptable
	↓ ↓ ↓ ↓ ↓
Overall Impact Assessment of activity loss	***5.0***

Adverse Impact Criteria: 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD / MAO*** = **Near Immediate Restoration Required**
Calculated ***Initial RTO*** = **Near Immediate Restoration Required**
MBCO = **A minimum level of operation which will guarantee the safety of air traffic services at XYZ International Airport**

Maximum anticipated (adverse) impact assessment immediately = **5**

EXAMPLE ONLY - Airport (Automated) Baggage System (ABS) - Fig **16**

BIA Template - Key Activities - ***Simplified*** *Version of* **Activity Impact Matrix** (Assuming airport operates 24H)

Activity & BIA Assigned Priority: Airport (XYZ Int'l Airport) ***AUTOMATED BAGGAGE SYSTEM*** - ABS - **MEDIUM** to **HIGH** Priority (e.g. 'Priority 1.5A; 1.5B etc.)

Risk: ***Complete loss of ABS facility*** (e.g. due ICT operating system failure). This '*risk*' would have been derived from a (separate) *RA*

Impact Durations →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
	↓	↓	↓	↓	↓
Overall Impact Assessment of activity loss	***2***	***3***	***3.5***	***4***	***4***

Adverse Impact Criteria: 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD / MAO***	= **18 hours**
Calculated ***Initial RTO***	= **9 hours** *(Note may require 'adjustment' after accounting for 'knock-on' effects of associated interdependencies [if any?])*
MBCO	= **50% recovery within 9 hours; 70% within 15 hours; 90% within 24 hours 100% within 24 hours**

Maximum anticipated (adverse) impact assessment beyond 30 to 36 hours outage = **4.25**

EXAMPLE ONLY - Airport based Ground Handling Agent - Departure Control System (DCS) - Fig **17**

BIA Template - Key Activities - ***Simplified** Version of* **Activity Impact Matrix** (Assuming airport operates 24H)

Activity & BIA Assigned Priority: Assigned GHA (XYZ Int'l Airport) ***Passenger Check-in*** - **MEDIUM** to **HIGH** Priority (e.g. 'Priority 1.5A; 1.5B etc.)

Risk: ***Complete loss of DCS*** (check-in system) ***facility*** (e.g. due software virus). This '*risk*' would have been derived from a (separate) *RA*

Impact Durations →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
	↓	↓	↓	↓	↓
Overall Impact Assessment of activity loss	***2***	***2.5***	***3***	***3.5***	***4***

Adverse Impact Criteria: 1 = Minor; 2 = Acceptable; 3 = Significant; 4 = Major / Serious / High; 5 = Catastrophic

Estimated ***MTPD / MAO***	= **18 hours**
Calculated ***Initial RTO***	= **9 hours** *(Note may require 'adjustment' after accounting for 'knock-on' effects of associated interdependencies [if any?])*
MBCO	= **50% recovery within 9 hours; 70% within 15 hours; 90% within 24 hours 100% within 26 hours**

Maximum anticipated (adverse) impact assessment beyond 30 to 36 hours outage = **4.25**

Note 1 - VERY IMPORTANT

At the bottom of each of figures 12 - 17 above will be found a sentence which looks something like:

'…………………… Maximum estimated impact beyond 36 hours outage = 4.25 ……………………'

This latter ***BIA derived 'worst case' IMPACT value*** (e.g. 4.25 in the example immediately above) is the one that you would need to use (as an input) during the associated ***risk*** management (***assessment*** / ***analysis***) procedure (see Section 5 / 2B / 3 [starts page 167])

More specifically it is the *impact **value*** to enter along the *'impact **arm**'* of the associated ***risk** matrix.* (You will recall that 'threat ***likelihood** / **probability***' values are entered along the ***OTHER*** matrix arm [the latter values being derived from the {***separate***} ***risk*** management / assessment / analysis itself])

Note 2

On each of figs. 12 to 17 above a '***priority for taking action***' level has been allocated (2nd line below top title)

If necessary (and particularly to avoid confusion), see again the 'important note' on page 155 regarding use of the same system of 'scores' etc. which might potentially be used for both **BC** and **RM** purposes - ***and thus the need to clearly understand the different context(s) in which they might be used***

Note 3

Referring to figures 12 - 17 above, page space constraints prevented adding of the following at the bottom of ***each*** figure:

BC Strategy Summary:	= *TBA (Note - in this guideline document the BC **Strategy** is documented at a later point [see Section **5.3** - starts page 197])*
Resources required:	= *TBA (Note - in this guideline the resources required to implement the BC Strategy are documented at a later point [see Section **5.3**])*
Interdependencies (Internal):	= *TBA (Note - these have been ignored for simplicity purposes. In reality they must, of course, be identified and accounted for)*
Interdependencies (External):	= *TBA (Note - these have been ignored for simplicity purposes. In reality they must, of course, be identified and accounted for)*

BIA - Review & Evaluation

Good practice indicates that a BIA be regularly reviewed (e.g. annually) - but also on an 'as required' basis in the event of e.g.

- Major change(s) to strategic business objectives
- Significant change(s) in internal business processes, location, technology etc.
- Significant change in the external environment, such as regulatory, market, supply chain change
- In conjunction with a new (risk management) assessment etc.

The BIA process should not be repeated in its entirety at review e.g. only specified key products / services / operations / activities / processes / procedures / dependencies / resources etc. affected by significant change need to be thoroughly reviewed

For evaluation / audit / compliance purposes, it is typically only necessary for nominated ***elements*** of the 'current' BIA to be periodically *'sampled and reviewed'* - together with confirmation that 'non-compliances' from previous BIA evaluations have been adequately addressed (corrective actions). Such 'sampling' should be managed e.g. in order that the entire BIA is eventually covered in an appropriate timescale e.g. 3 to 5 yearly for the larger / more complex organisation - before restarting the sampling cycle again

ISO 22317 - 2015

An additional ISO 'Business Continuity' related 'Technical Specification' (TS) was released in 2015 - being ISO 22317: 2015 - 'Guidelines for **Business Impact Analysis** (BIA)'

A good idea - but practically not anything like as useful it ought to have been (i.e. a similar situation to all of the other ISO Business Continuity related 'Standards' and their 'Technical Specification' supporting documents - as expanded upon in Note 4 [starts on page 33] of ***separate* but related** guideline document in ***this*** series - 'CRPM Part 3 / Volume **1**.

If you have reason to doubt what has been written just above - also take a look at the info found at the end of the below link (and 'read between the lines' what the BC expert author is really trying to say - albeit very diplomatically!!!)

https://www.continuitycentral.com/index.php/news/business-continuity-news/529-the-new-iso-ts22317?tmpl=component

Section 5 / **2B / 3**

> Reminder: In *this* guideline the ***BIA*** was addressed first before we moved on to (now) look at the ***RA***. There is, however, no reason why this sequence cannot be changed. There are no particular advantages / disadvantages to both but, if completed correctly, the end result should be the same, for any set of given circumstances

Risk Assessment (including Risk Analysis)

See again Notes 1 & 2 on page 130. Also see *risk related* definitions now - pages 170 to 172

Reminder 1 - Risk Assessment is a component of the overarching Risk Management process

Reminder 2 - Risk Management *versus* Business Continuity (see next 5 paragraphs below)

It will be recalled that risk management (RM) **is the practice of an organisation systematically identifying, selecting and managing various processes designed to avoid / minimise / mitigate etc. the** (typically) **adverse effects of threat realisation** (i.e. of a threat actually occurring) **to one or more of its activities** (products / services / operations etc.)

As threats can never be fully avoided or mitigated, organisations will always need to accept some level of risk. Indeed, we have already seen earlier in this guideline that certain risks are sometimes taken by organisations in a calculated / reasoned ‘gamble’ (Risk Appetite) that some form of advantage will result (typically [but not always] finance related)

Whereas RM tends to be pre-emptive, business continuity management (BCM) was ‘invented’ to deal with the continuity consequences of a realised threat(s) - i.e. ***AFTER*** it has actually occurred

RM and BCM are often mistakenly seen as ‘rivals’. In fact, the two are so closely interwoven that such separation is academic. For example, the risk management process creates important inputs for BCM (e.g. identification of assets [resources such as people, equipment, facilities etc.], threat impact assessments, cost estimates …………… and so on)

RM also proposes applicable controls (treatments) for identified risks - one of which ***MIGHT*** (repeat: ‘MIGHT’) be via use of ***BC*** measures. Therefore, risk management covers several areas which are vital for the BCM process and even (in fact) for its existence. However, the BCP process itself goes beyond RM's ***pre-emptive*** approach and assumes that the ‘disruptive incident’ ***will*** actually happen at some point - and so we get the questions ‘what happens then / what do we do now’ etc?

General

Typical threats to organisations include those which have the potential capability to (list is not exhaustive):

- Damage property and / or people e.g. fire, flood, earthquake, hurricane, tornado, volcanic eruption, terrorism / bomb etc.
- Prevent people from working e.g. sickness, industrial action, transportation stoppages
- Cause loss of systems, networks and similar type scenarios
- Cause failure of key supply systems etc.
- Damage brand / image / reputation etc.

Organisations should identify, understand and document potential threats which (if realised) might have both a sufficiently adverse ***impact*** (on the organisation - or more specifically on its business activities, processes, resources, dependencies [including suppliers], brand / image / reputation etc.) to be worthy of consideration .... **+** also have a sufficiently high degree of ***likelihood / probability*** of occurrence

Identified threats should be ***regularly reviewed*** in order to validate / change any already assigned likelihood and / or impact assessments. The organisation should also periodically look for and add (as applicable) any new / emerging threats. For example, it is only relatively recently that many organisations (including airlines and airports etc.) have needed to account for the threat (epidemic and pandemic) of communicable disease. (See also ***separate*** [but related] document CRPM Part 3 / Volume **1** - appendix B [Horizon Scanning])

For example, in 2019 - 2020 '* ***pandemic***' (along with ICT related vulnerabilities / cyber-crime, terrorism / sabotage and the 'weather / natural phenomenon' [e.g. global warming {albeit caused by humans}]) was high on most national, regional and local government threat lists (otherwise known as ***risk registers***)

Risk registers also apply to (should be used by) all types of aviation related organisations - and rightly so considering the potentially disastrous human and financial consequences should certain potential threats be realised

** It is suggested that the best way to identify which specific threats might occur - to which specific activities - for a particular organisation - is probably during the interviews / workshops / questionnaires etc. deployed during the ***BIA*** - as the associated subject matter experts (contributing to the BIA) will also be typically (but not always) best placed to both identify such threats and to assess their ***likelihood / probability*** of occurrence

The results are fed into the associated risk assessment (RA) process (pedantically separate from the BIA process but practically speaking almost integral) - and the same subject matter experts consulted once again to ensure that the conclusions of the RA are as practically / realistically 'correct' as possible

* Rightly so as in December 2019 the COVID-19 pandemic originated in China and rapidly spread around the world e.g. by late May 2020 around 5.5 million infections might have occurred with 400,000 associated deaths (and the pandemic was 'still going strong' at that point). For a number of valid reasons it is anticipated that said infections / deaths are ***very significant underestimates*** of the real figures

** If the organisation ***already*** has an established Risk Management (RM) department / business unit, then (assuming that they have done their job competently and thoroughly) most risks which are significant to the organisation should already be known, documented and been controlled / treated etc. However, in ***this*** guideline document we are assuming that there is ***no*** formal ***Business Continuity*** capability ***yet*** established within that same organisation - which means (we assume herein) that the specific ***risk*** control / treatment (which should relate directly to the application of ***BC*** measures) will either have **not** been addressed at all - or been addressed in an **inadequate** manner

(If the content of the last para was ***not*** the case, then the RM department / business unit [if it exists] had, effectively, ***also*** become the 'de facto' BC department / business unit! i.e. two departments in one)

As this guideline document is all about establishing a BC capability - and we are assuming that the organisation's RM department / business unit has not yet adequately addressed this particular subject (BC) - for whatever reason (again, including the possibility that an RM department / business unit ***does not exist***), it will be necessary to fully incorporate the latter unit (***OR*** its equivalent accountabilities i.e. as if it ***did*** exist) into the BC 'understanding the organisation' task

For example, the RM business unit may have missed out some key activities from its risk assessments - which have now been identified by the BIA. Conversely, there may be activities included in the RA which should have also been included in the BIA - but were missed for whatever reason

Furthermore, the RM business unit will have (should have) previously / already come up with its own '***impact***' ratings for the ***consequences*** of a particular ***threat*** on a particular ***activity***. These now need to be re-assessed in light of the 'impact' ratings ***derived from the BIA*** - which will probably be more valid than those found in any previous RA conducted by the RM business unit itself

It is these latter re-assessed impacts (derived from the *** BIA and **not** the RA) which now need to be re-entered into the appropriate risk matrices (as related to particular threats and activities) - and previous risk level assessments either confirmed and / or corrected

*** See again the 'very important notes' on page 165

Many activities (selected from the BIA as being 'significant' from a BC viewpoint) will, by their nature, typically sit in the 'low to medium low ***likelihood***' / 'high to extremely high ***impact***' section of the associated risk matrix. If the ***likelihood*** of a threat occurring is considered to be greater than this and the threat has not yet been addressed by the organisation - then something has probably gone quite badly wrong somewhere at some time - and associated urgent attention required!

Lastly, most aviation related organisations associated in some significant way with flight operations (*e.g. aircraft operators, airport operators, GHAs, MROs, air navigation service providers, flight training organisations, appropriate government departments etc.*) are legally (*or similar compulsion e.g. regulatory*) required to conduct risk assessments on all 'operational' safety related activities (strangely enough known as ***'operational*** or ***safety RISK** assessment'* [See page 180])

It ***is*** remotely possible that such operational / safety risk assessments might be undertaken by an organisation's RM department / business unit (if it has one?). However, such assessments are far more likely to be undertaken by the organisation's ***flight safety manager*** or equivalent person. Regardless, the results are available for use (***and should be so used where applicable***) in the ***appropriate*** parts of the 'understanding the organisation' task e.g. in the **BIA**

IMPORTANT - if no ***formal*** **RM** capability exists within an organisation, top management should decide on and approve (including budget where required) an appropriate course of action. Options include:

- Establishing a ***formal*** **RM** department / business unit in its own right (which may or may not ***also*** be required to formally assume ***BC matters*** in full)
- Assign **RM** type duties (specifically as they impact on ***formal BC type matter***s ***but nothing else***) to the BC department / business unit. This effectively means that ***other*** required RM capabilities / accountabilities etc. will not be available to the organisation
- Appoint an appropriate, external (subject matter) expert to look after the organisation's RM requirements (budget accordingly required)
- Do nothing. Of course, this is not an option at all if the organisation is serious about the introduction of a BCMS

Some Simplified Definitions

Threat

Something bad that might happen (to something, someone)

Threats can range from innocent (to not so innocent) mistakes made by employees - to natural disasters - to terrorist / sabotage activities - to IT hacks and viruses - to industrial action - to pandemic - to economic depression - to a nuclear power station meltdown - even (e.g. in the case of airline and airport operations) to bad weather (snow & ice closing an airport to flight operations) and volcanic eruptions ……………… to name just some

Whilst it is possible to identify most threats against a specific something / someone - it is impossible to identify ***all*** threats

Note - where considered helpful, ***threats*** might be listed under categories into which they might best fit e.g. natural, human, technological / environmental etc. For examples see figure 18 - starts on page 173

Vulnerability

Exposure to a threat(s)

For example, fire in a facility is a threat

Associated ***vulnerabilities*** which might enable the threat to be realised (to actually happen) include e.g. no alarm system; lack of fire extinguishers; no other fire suppressant system(s) (e.g. sprinklers); no fire doors; no associated training; no associated fire drills conducted; no associated fire-drill / fire exit signs & instructions etc.

In a common aviation context, lack of snow & ice clearing resources is a (one) ***vulnerability*** with respect to the associated ***threat*** of snow / ice closing an airport. If snow & ice clearing equipment resources ***are*** available, then lack of competent and experienced human operators might be a different vulnerability ……………………… and so on

Note - where considered helpful, ***vulnerabilities*** might be organised / grouped with regard to the activities, processes and resources to which they best relate e.g. ***hardware*** and ***equipment*** (unavailability; lack of maintenance; not fit for purpose), ***ICT*** (too complex; no control over data input; insufficient server capacity; inadequately protected), ***services*** (lack of security clauses in contracts, lack of supply chain oversight; lack of service level agreements), ***information*** [digital] (zero or insufficient access control, zero or insufficient backup), ***information*** [hard copy] (no physical protection, inadequate document control), ***infrastructure*** (lack of physical access control, inadequate fire protection), ***human resources*** (inadequate training and exercising, lack of manpower) etc.

Risk

Evaluation of the *likelihood* of a *threat* and its associated *vulnerabilities* on something or someone (the latter being the subject of the threat) **- which, when combined with the *impact* of the threat should it actually occur** (be realised) **= the RISK on / to that something / someone - as related to that threat**

……………..or (arguably), and perhaps a little more clearly:

Any internal or external situation / event having the *potential* to impact upon an organisation - which might (if realised) **prevent the latter from successfully achieving its business objectives; capitalising on its opportunities etc.**

By its very nature risk is neither precise nor scientific i.e. it is a subjective matter by default e.g. at commercial airports which are subject to fairly heavy snow fall / ice formation on a regular (seasonal chance) basis - the lack of appropriate snow / ice clearing resources (deliberate or otherwise) may be seen as a high risk situation / decision. If the airport closes down for a significant period every time that there is snow / ice - then customers are going to go elsewhere (if there is an elsewhere), and the airport might go out of business

Taking the same situation but changing the seasonal chance of heavy snow / ice to e.g. once every 20 years (e.g. as might be extrapolated from statistical meteorological data for any particular airport) - then the risk of associated airport closure might be seen as being so (relatively) low, that it is * not worth investing in the very expensive snow and ice clearing equipment & resources which ***would*** be needed in the circumstances described in the paragraph immediately above

The above is thus an example of where 'risk / threat' evaluation process can save money - and so, perhaps paradoxically, risk might be considered to be 'attractive' - depending on the circumstances (see glossary [CRPM Part 3 - Volume 1] for definition of '***risk appetite***')

* Note - in this example situation the airport should not actually be so cavalier as to have absolutely no snow / ice clearing capability / response at all e.g. more basic (hence cheaper) snow / ice clearing equipment may be held. Insurance against airport closure due snow / ice could also be taken out to at least recover financial losses etc. (Both being known in risk management terminology as 'risk **controls**' or 'risk **treatments**' or risk '**solutions**' etc.)

Managing risk as described above is, logically enough, known as *'risk management'*

Risk Management

The process of systematically identifying & understanding risk (to the organisation) **- together with application of the associated controls** (solutions / treatments / measures etc.) **put in place to manage same**

This process ultimately leads to the decision of whether (in the context of a particular organisational activity / function) a specific risk is acceptable or requires further action to reduce the (generally) adverse consequences of what it (that specific risk) is capable of impacting upon

Threats / Threat **Categories** / Threat **Associated Vulnerabilities & Consequences**

Referring to figure 18 on the next page ……………………

- The images on the far left represent a ***pictorial*** sample of some of the ***more typical*** **threats** to ***most*** organisations (there are many more of course)

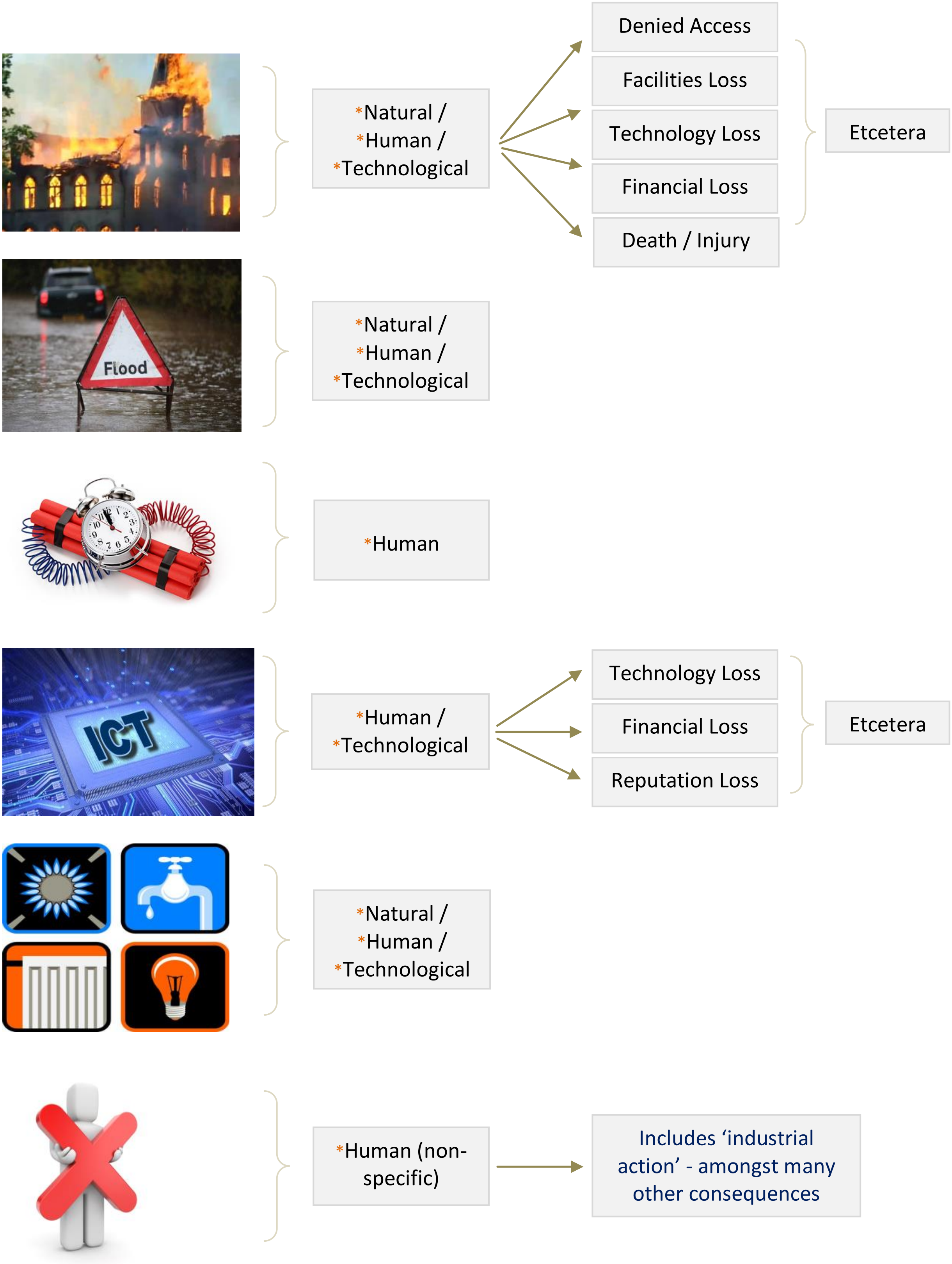
- The ***first*** 'text box' to the ***right*** of the images provides ***typical*** **categories** into which a ***particular*** threat might be assigned / belongs. This is not a precise matter as a specific threat can sit in several different categories, depending on the context of what it is it threatens - and how. Thus several possible example categories might be included / shown (per threat) for consideration - as applicable

- The ***next*** text box to the right indicates (for ***some*** of the threats & thus for example purposes only) ***some*** of the typical **consequences** …………… should the threat be realised (see also 'RA Triggers' - starts bottom of page 178)

- Space constraints in figure 18 prevent insertion of the potential **vulnerabilities** which are typically associated with each threat. However (and as an already mentioned example), the threat of fire to a facility is generally associated with the following typical ***vulnerabilities*** (the list is not exhaustive):

  - No fire suppressant (e.g. sprinkler) system in place
  - No fire doors
  - No fire extinguishers
  - No 'in the event of fire' instructions
  - No associated training
  - No fire drills scheduled etc.

Figure **18**



*Natural / *Human / *Technological → Denied Access / Facilities Loss / Technology Loss / Financial Loss / Death / Injury → Etcetera

*Natural / *Human / *Technological

*Human

*Human / *Technological → Technology Loss / Financial Loss / Reputation Loss → Etcetera

*Natural / *Human / *Technological

*Human (non-specific) → Includes ‘industrial action’ - amongst many other consequences

Figure 18 - continued

*Natural /
*Human /
*Technological

Financial Loss

Reputation Loss

Etcetera

*Natural /
*Human

*Human

*Natural

Technology Loss

Denied Access

Financial Loss

Reputation Loss

Technology Loss

Death / Injury

Etcetera

*Natural /
*Human /
*Technological

*Human

Risk Management Process / Methodology - Simplified Summary

- * Identify and document what it is (key activity etc.) that requires to be protected against threats
- ** Identify and document the ***threats*** to each and every such key activity etc.
- Assess and document the ***vulnerabilities*** of each such key activity etc. as related to ***each identified and associated threat***
- Determine the ***risk*** (i.e. the **evaluation** [***analysis***] of expected ***likelihood*** [probability] versus ***impact*** [as related to associated consequences]) of each identified threat on each such key activity etc.
- Assess ***the resulting risks*** to see if they can be accepted by the business without further attention. Document the results for those that can
- *** For those risks which require further attention (because they have been assessed as having some degree of 'unacceptability' during the above analysis) - identify methods (strategies and tactical solutions) for reducing (mitigating / managing / controlling / treating) the likelihood and impacts of each such risk on each such activity. Document the results
- Prioritize risk reduction measures based on an associated strategy
- ***Make it all happen***
- Continually monitor and evaluate all of the above
- Cyclically review / monitor / maintain etc. all of the above
- Retain and maintain documented records where appropriate

* This information is derived from the associated BIA

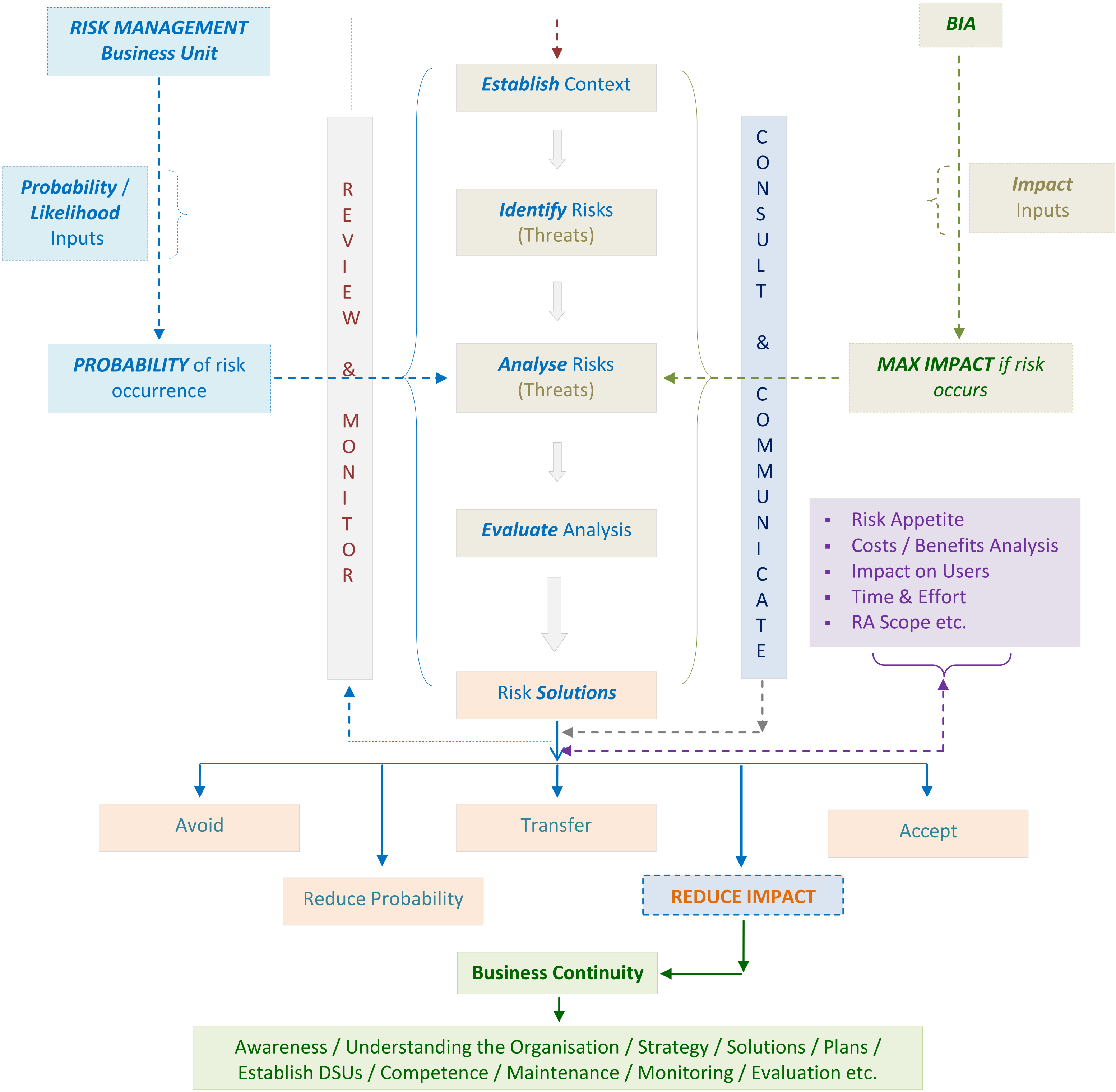
** Pedantically known as a 'threat assessment'

*** Reminder - one (but just one) of several ***risk*** mitigation / management methods available is to use ***business continuity*** measures (e.g. Understanding the Organisation; Selecting BC Strategy and (associated) BC Tactical Solutions; Preparing BC Plans; Set-up, training, exercising and operation of 'Disruption Support Units' etc.)

Note 1 - see figure 19 on the next page for a diagrammatic version of the above

Note 2 - the above is a ***very*** simplified 'methodology' for risk assessment. For 'hints' as to how it might be more formally accomplished, you might consider using the BIA type 'methodology' (starts page 141) as an approximate template

Risk Management (Assessment [Analysis]) **Process**



RISK MANAGEMENT* *Business Unit

Probability / Likelihood Inputs

PROBABILITY of risk occurrence

REVIEW & MONITOR

Establish Context

Identify Risks (Threats)

Analyse Risks (Threats)

Evaluate Analysis

Risk ***Solutions***

CONSULT & COMMUNICATE

BIA

Impact Inputs

MAX IMPACT *if risk occurs*

- Risk Appetite
- Costs / Benefits Analysis
- Impact on Users
- Time & Effort
- RA Scope etc.

Avoid

Reduce Probability

Transfer

REDUCE IMPACT

Accept

Business Continuity

Awareness / Understanding the Organisation / Strategy / Solutions / Plans / Establish DSUs / Competence / Maintenance / Monitoring / Evaluation etc.

Figure 19

Assessing Risk

There are several methods used to assess / evaluate (***analyse*** [quantify / qualify]) risk (none of which is perfect due the subjective nature of the topic). Perhaps the most widely used method (due its relative simplicity) uses the following parameters:

Assessed Risk = ***Impact*** of ***threat*** event x (multiplied by) ***probability*** of ***threat occurring***

The ***impact*** of a specific threat event (should such threat be realised) upon a specific activity is typically assessed on a scale of 1 to 5, where 1 and 5 represent the minimum (typically ‘negligible’) and maximum (typically ‘catastrophic’) possible impacts respectively

The ***probability*** (likelihood) of a specific threat event being realised on a specific activity is likewise commonly assessed on a scale from 1 to 5 (or, alternatively, use an A to E scale to assist is differentiating the ***impact*** arm of the risk matrix from the ***probability*** arm), ***where 1*** *(or A)* ***= almost certain not to occur***………………… and ***5*** *(or E)* ***= almost certain to occur***

These probability related numbers / letters may be linked to ‘units of time’ type terminology if required (e.g. event occurs once a year, once in ten years, once in 100 years etc.) or may also be expressed in "plain english" (e.g. event occurs often; event occurs rarely etc.)

The scales referred to above can be linear or non-linear depending on decisions made by the appropriate subject-matter experts, regarding the specific activity and the specific threat under consideration - and also as related to how the risk assessment might best be derived from the matrix

The ‘***assessed risk***’ can thus take values ranging from * **1** (1 x 1) **to 25** (5 x 5). It is common for this range to be sub-divided into three (or possibly more) further ‘sub-ranges’. The overall risk assessment is then typically rated Low, Medium or High, depending on the number values contained in ***each*** sub-range e.g. numbers 1 to 5 might equate to a ***low*** risk; 6 to 12 might equate to ***medium*** risk …………..with 13 to 25 being reserved for ***high*** risk

* Or e.g. **1A** to **5E** if using the alpha / numeric system referred to further above (see also Figs. **20D**, **20E** and **20F** - starting on page 184)

The appropriate subject matter experts will generally be the best persons to decide which numbers fall into which sub-range - and also what the ***specific*** numbers actually mean in plain language - as related to the specific activity and the specific threat

A more meaningful terminology (as related to the above) might e.g. be:

1 to 5 = **Acceptable Risk** i.e. we either do not need to manage this risk at all OR…………………… if we do decide to manage it (for whatever valid reason) - the controls / treatments applied are likely to be low key, inexpensive and use minimal resources - and to also be applied in the longer term. Managed by the activity owner

6 to 12 = **Unacceptable Risk** - robust controls / treatments are required to bring the risk into the acceptable category within the shorter to medium term timescale. Managed by the activity owner - with regular oversight provided by the appropriate senior manager (typically graded as Director / Senior Vice President / equivalent)

13 to 25 = **Unacceptable Risk** - the organisation's top management (e.g. Board of Directors) will decide if the associated activity is to be continued or discontinued

If the former, the strictest and most comprehensive controls / treatments must be applied in the immediate shorter term, in order to bring the risk into the acceptable category

Anything scoring a 5 for ***'impact'*** ***requires specific review in its own right*** - ***regardless*** of the associated 'probability / likelihood' score

Note 1 - instead of using an 'odd' number of numbers (e.g. 1 to 5 as outlined above) and similar - consider using an 'even' number of numbers / similar instead (e.g. 1 to 6; A to F etc.). This assists in preventing 'assessors' from the undesirable but common temptation of 'sitting on the *middle number / middle letter*' fence' (i.e. the number '3' in the 1 to 5 scale'; the letter 'C' in the A to E scale etc.)

Note 2 - For any particular activity, the evaluation of **RA *likelihoods / probabilities*** and the associated ***impacts*** should be assessed on the risk which would exist if all preventative or mitigating controls (i.e. those which may ***already*** be in place ***before*** the RA is conducted**) are discounted / ignored**

The eventual risk solutions / treatments / controls resulting from the 'new' RA are then established - and will more than likely (but not always) ** confirm that the 'already in place' solutions etc. are still valid / required - and may possibly also identify the need to add additional solutions etc.

** For example, when the nature of the activity in question (and / or the associated threats) has changed significantly since the last RA

Note 3 - the level of risk remaining ***after*** solutions etc. have been applied (there will ***always*** be some such risk) is typically known as **'residual risk'**. The latter is generally (but not always) acceptable to the organisation. Should it ***not*** be acceptable, further solutions etc. should be applied until it does become acceptable (If the latter is unachievable, ***then the activity will probably need to cease***)

RA Triggers

To better manage and organise the RA process and to facilitate what is to follow on (i.e. selection of appropriate RA solutions / treatments / controls - one of which is assumed [in this guideline document] ***to require use of BC measures***) it is suggested that a structured approach might consider use of *'RA Triggers'* covering a ***range*** of associated threat consequences

As an example consider the impacts / consequences during peak 'work' travel commute times of e.g. a transport strike; burst water main; terrorist attack; snow and ice etc. - which has resulted in denied access to an organisation's only / main premises

The RA trigger which covers ***this*** particular eventuality might ***generically*** be entitled:

'Denied Access to Organisation's Premises'

Each trigger could be 'tripped' by one or more threats. Similarly a specific threat might 'trip' one or more triggers

Organisations can typically 'boil down' the trigger list to around ten or fewer components e.g. as typically related to variations in loss of premises, staff, equipment, systems, key suppliers, money, reputation, shareholder confidence, death / injury etc.

Whenever a new threat is identified, it is included within the most appropriate existing trigger (or, where appropriate [rarely if the preparation has been good] by creating a new trigger)

The ***likelihood*** of the trigger being tripped is the sum of the likelihood of all the threats (that the trigger is associated with) being realised. The ***importance*** (priority) assigned to each RA trigger might be determined using ***BIA*** derived results

Determining how the organisation should respond to each trigger (if tripped) will essentially define the organisation's ***business continuity strategy*** (and its ***risk strategy*** also of course - but the latter is beyond the scope of this guideline document - except for its associated BC component)

Example of a Real (Aviation Related) **Risk Assessment Process**

* We can now look at a generic example (see pages 180 to 186 below) of how RA works in practice - by taking the subject of '***operational*** (safety) ***risk assessment***' e.g. within an airline, an airport etc.

In this example we will look specifically at the aviation related concept and activity known herein as '***operational safety***' (more formally known in the aviation context as simply 'Safety Management')

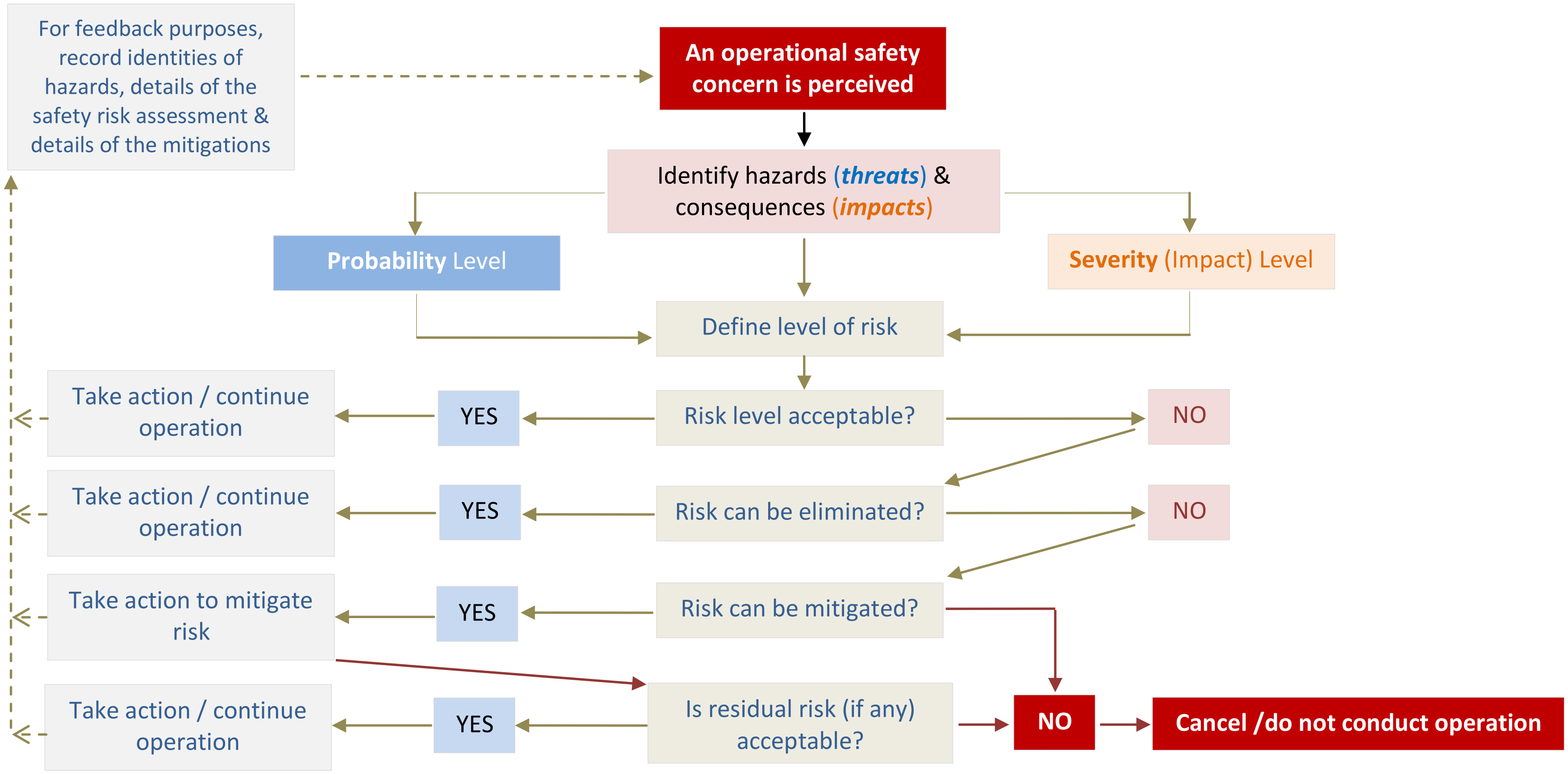
* Taken from ICAO **Safety Management Manual** - SMM (Doc 9859 - 4th Edition - 2018)

See page 169 of ***this*** guideline document (fifth para from the top) for what type of aviation related organisations typically fall under the umbrella of '***operational safety risk assessment***'. It is important to note that the ***principles*** of operational safety also ***apply equally to all other activities within such organisations - which are not 'normally' classified as 'operational' e.g. HR, Finance etc.***

Note - as at 2020, all (UN member) countries of the world (i.e. governments) + their major ***aviation*** related organisations needed to comply with the requirements of the International Civil Aviation Organisation's (ICAO) ***Safety Management System*** - '**SMS**'

A simplistic flowchart of how the latter 'works' is shown on the next page

Figure **20A** - **Operational Safety - Risk Management** (*Activity* = SAFETY) (This page © ICAO)



For feedback purposes, record identities of hazards, details of the safety risk assessment & details of the mitigations

An operational safety concern is perceived

Identify hazards (***threats***) & consequences (***impacts***)

Probability Level

Severity (Impact) Level

Define level of risk

Risk level acceptable?

YES

Take action / continue operation

NO

Risk can be eliminated?

YES

Take action / continue operation

NO

Risk can be mitigated?

YES

Take action to mitigate risk

Is residual risk (if any) acceptable?

YES

Take action / continue operation

NO

Cancel /do not conduct operation

Examples - continued

OPERATIONAL SAFETY - RISK MANAGEMENT (This page © ICAO)

Safety Risk Management (SRM) is a key component of overall safety management and includes hazard identification, safety risk assessment, safety risk mitigation and risk acceptance

Here we present the fundamentals of safety risk under the following topics and information:

- A definition of 'hazard'
- A definition of 'safety risk'
- Safety risk probability
- Safety risk severity
- Safety risk assessment
- Safety risk tolerability

Definition - 'Hazard'

A condition or an object having the potential to cause or contribute to an ***aircraft incident or accident***

Definition - 'Safety Risk'

Safety Risk is based on the predicted probability (likelihood) and severity (impact) of the consequence(s) or outcome(s) of / from a realised hazard (or equivalent situation). Whilst a predicted consequence / outcome ***may*** in the worst case relate e.g. to an aircraft accident, an 'intermediate unsafe event' is statistically more likely to be the actual situation 'on the day'

Safety Risk Probability

The process of controlling safety risk starts by assessing the ***probability*** that the ***consequences*** of ***hazards*** will materialize during aviation activities performed by the organisation. Safety risk probability is defined as ***'..............the likelihood that a safety consequence or outcome will occur............'*** The determination of likelihood can be aided by questions such as:

- Is there a history of occurrences similar to the one under consideration - or is this an isolated occurrence?
- What other equipment, components etc. of the same type might have similar issues?
- How many persons are following (or subject to) the procedures (activities) in question?
- What percentage of time is the suspect equipment or questionable procedure in use?

Any factors underlying these questions will help in assessing the likelihood that a hazard may exist, ***taking into consideration any foreseeable scenario***. The determination of likelihood can then be used to ***assist*** in determining safety risk ***probability***

Examples - continued (This page © ICAO)

Figure 20B below shows a typical safety risk ***probability*** table. It includes five categories for denoting the probability of occurrence related to an unspecified, unsafe event or condition, the description of each category, and an assignment of a value or 'score' to each category

It must be stressed that this is an example only and that the level of detail and complexity of tables and matrices should be adapted so as to be commensurate with the particular needs and complexities of the organisation

Also, note that organisations can include both qualitative & quantitative criteria in such tables

Probability	Meaning	Value
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur - but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely Improbable	Almost inconceivable that event will occur	1

Figure **20B** - Safety Risk Probability Table

Safety Risk Severity

Once the ***probability*** assessment has been completed, the next step is to assess the safety risk severity (***impact***), taking into account the potential consequences related to the hazard

Safety risk 'severity' is defined as *'.............................. **the extent** (amount etc) **of harm which MIGHT reasonably be expected to occur as a consequence / outcome of a particular, identified hazard occurring**.........................'*
The severity assessment can be based upon parameters such as:

- Fatalities / injuries. How many lives may be potentially lost (employees, passengers, bystanders, the general public etc.)?
- Damage. What is the likely extent of damage to aircraft, property, infrastructure etc.?

The severity assessment should consider all possible consequences related to a hazard, taking into account the worst foreseeable situations

Figure 20C on the next page presents a typical safety risk severity table. It includes five categories to denote the level of severity, the description of each category and the assignment of a value to each category

As with the safety risk probability table, this table is an example only

Examples - continued (This page © ICAO)

Severity (Impact)	**Meaning**	**Value**
Catastrophic	▪ Multiple Deaths ▪ Severe Destruction of Property, Infrastructure etc.	A
Hazardous	▪ A large reduction in Safety Margins ▪ Physical Distress ▪ Workload such that operators cannot be relied upon to perform tasks accurately and / or completely ▪ Serious Injury ▪ Major Damage to Property, Infrastructure etc.	B
Major	▪ A significant reduction in Safety Margins ▪ Workload (or other efficiency impairing condition(s)) - such that operators suffer a reduction in ability to cope with adverse operating conditions ▪ Serious Incident ▪ Injury to Persons	C
Minor	▪ Nuisance ▪ Operating Limitations ▪ Use of Incident Procedures ▪ Incident (not serious)	D
Negligible	▪ Few consequences (none serious)	E

Figure **20C** - Safety Risk Severity (Impact) Table

Safety Risk Assessment

The safety risk ***probability*** and ***severity*** assessment process used to derive a ***safety risk index***

The index created via the methodology described (in the tables above) above consists of an alphanumeric designator, indicating the ***combined*** results of the probability and severity assessments

The respective severity / probability combinations are presented in the safety risk assessment matrix - as shown in the figure 20D on the next page

Examples - continued (This table © ICAO)

Risk PROBABILITY	Risk Severity **(IMPACT)**				
	(Catastrophic) **A**	(Hazardous) **B**	(Major) **C**	(Minor) **D**	(Negligible) **E**
5 (Frequent)	**5A**	**5B**	**5C**	**5D**	**5E**
4 (Occasional)	**4A**	**4B**	**4C**	**4D**	**4E**
3 (Rare)	**3A**	**3B**	**3C**	**3D**	**3E**
2 (Unlikely)	**2A**	**2B**	**2C**	**2D**	**2E**
1 (V. Unlikely)	**1A**	**1B**	**1C**	**1D**	**1E**

Figure **20D** - Safety Risk Assessment Matrix

Safety Risk 'Tolerability'

The last step in the process is to determine safety risk ***tolerability***

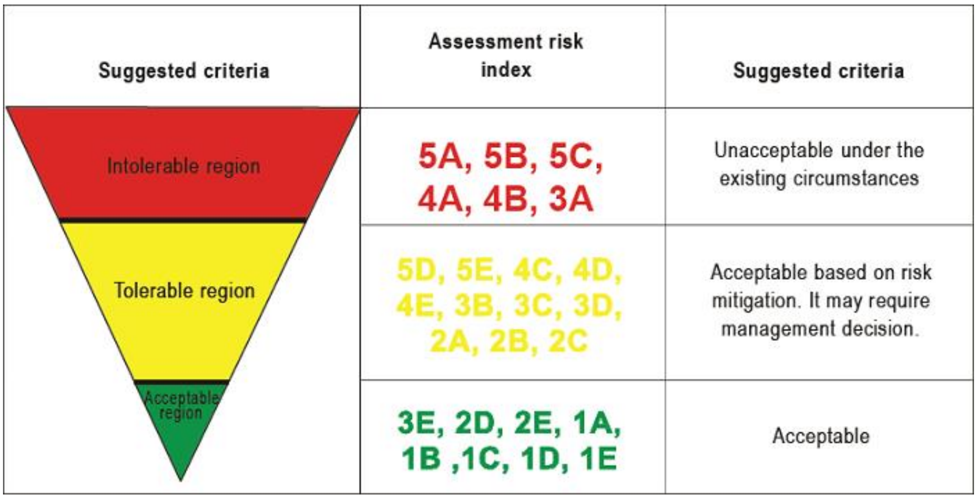
Firstly, obtain the 'indices' from the figure 20D above. For example, consider a particular ***situation*** where a safety risk probability has been assessed as occasional (**4**) - and safety risk severity / impact etc. has been assessed as hazardous (**B**). The composite of probability and severity (**4B**) is thus the ***safety risk index*** of the ***consequences*** for this ***particular situation***

The resulting safety risk index is then 'exported' to a safety risk ***tolerability*** matrix (see figures 20E & 20F on next page) which describes the ***tolerability*** criteria for the particular organisation in question

Using the example above, the criterion for a safety risk index value assessed as **4B** falls in the **'unacceptable under the existing circumstances'** category. The organisation must therefore:

- Reduce the probability / likelihood component of the risk index to an acceptable level……………………………and / or
- Reduce the severity component of the risk index to an acceptable level……………………………or
- Reduce both of the above so that the risk is managed to an acceptable level ………………..or
- Cancel the operation (particular situation) if mitigation (reduction) to an acceptable level is not possible

Examples - continued (Below diagrams © ICAO)



Suggested criteria	Assessment risk index	Suggested criteria
Intolerable region	5A, 5B, 5C, 4A, 4B, 3A	Unacceptable under the existing circumstances
Tolerable region	5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Acceptable based on risk mitigation. It may require management decision.
Acceptable region	3E, 2D, 2E, 1A, 1B ,1C, 1D, 1E	Acceptable

Figure **20E** - One Model of a Safety Risk Tolerability Matrix

Risk Assessment/Index Range	Risk Description	Recommended Action
5A, 5B, 5C 4A, 4B, 3A	INTOLERABLE	Take immediate action to mitigate the risk or stop the activity. Perform priority safety risk mitigation to ensure additional or enhanced preventative controls are in place to bring down the safety risk index to tolerable
5D, 5E, 4C, 4D 4E, 3B, 3C, 3D 2A, 2B, 2C	TOLERABLE	Can be tolerated based on the safety risk mitigation. It may require a management decision to accept the risk
3E, 2D, 2E, 1A 1B, 1C, 1D, 1E	ACCEPTABLE	Acceptable. No further safety risk mitigation required

Figure **20F** ………………………………………and another model - complete with recommended actions

Examples - continued

In the next example (which is ***real***) we are looking at a specific threat against a specific airline's operation

The threat was that of a * sub-sea 'earthquake initiated' ***Tsunami*** which needed to be accounted for (controlled / treated) by the airline concerned as the consequences (should the threat be realised) to its deployed staff (i.e. pilots, cabin crew, engineers and other operational staff located in the potential Tsunami geographic region) and resources (particularly aircraft) could be potentially catastrophic (score of '5' on a 1 to 5 scale) - albeit (regardless of the fact) that the eventual outcome of the risk assessment gave a likelihood / probability score of extremely low ('1' on a 1 to 5 scale)

* Similar to the infamous Tsunami of 26 December 2004 which is estimated to have killed around 250,000+ persons

The airline's operation in 2009 (which is the subject of this example) was ground based in the same part of the world as where this real Tsunami originated

It will be recalled from page 178 that a threat impact of '5' must be managed / mitigated ***regardless of*** the associated likelihood / probability score

The airline concerned had deployed (from its home base in Europe) several aircraft plus operating crews and supporting staff - to airports serving 3 different Indonesian cities - to assist the national airline with the annual requirement of flying Indonesian based pilgrims to and from Saudi Arabia for the Hajj (holy pilgrimage to Mecca)

See now the related information shown on the next two pages (taken directly from the above airline's 'risk register' at the time):

Examples - continued

Extract from a typical airline's RISK REGISTER (showing a typical Risk Matrix)

(Wet leased) **FLIGHT OPS CONNECTED WITH 20xx HAJJ from INDONESIA to S. ARABIA**

Activity / Resource / Threat: *HAJJ / Deployed Staff / Tsunami*

Risk Description

X - *Unable to expeditiously evacuate staff in event of tsunami*. **Y** - *Due to the unpredictability and potentially devastating effects of same*. **Z** - *Resulting in potential death or injury to staff*

Impact

Potentially very hazardous to catastrophic (in terms of people) [but see 'note 1 - next page]

Likelihood

Should a major sub-sea earthquake occur in the sea area east of Sumatra and / or north of Java, the ***potential*** for ***tsunami*** could relate to an ***extremely hazardous* to *catastrophic*** situation at Balikpapan operating base (both at airport and city) and at Banjarmasin operating base (city only). Staff accommodation (HOTAC) is assumed to be city based

Airport or City	Impact Rating	Likelihood Rating	Risk Rating
Batam City	2	1	**2**
Batam Airport	2	1	**2**
Balikpapan City	5	1	**5**
Balikpapan Airport	5	1	**5**
Banjarmasin City	5	1	**5**
Banjarmasin Apt	2	1	**2**

Note - above matrix is based on an impact scale of 1 to 5 - and a likelihood (probability) scale of 1 to 4. To estimate the ***risk*** rating - the impact and likelihood ratings have been ***multiplied***

Action Plan (Risk Treatment[s])

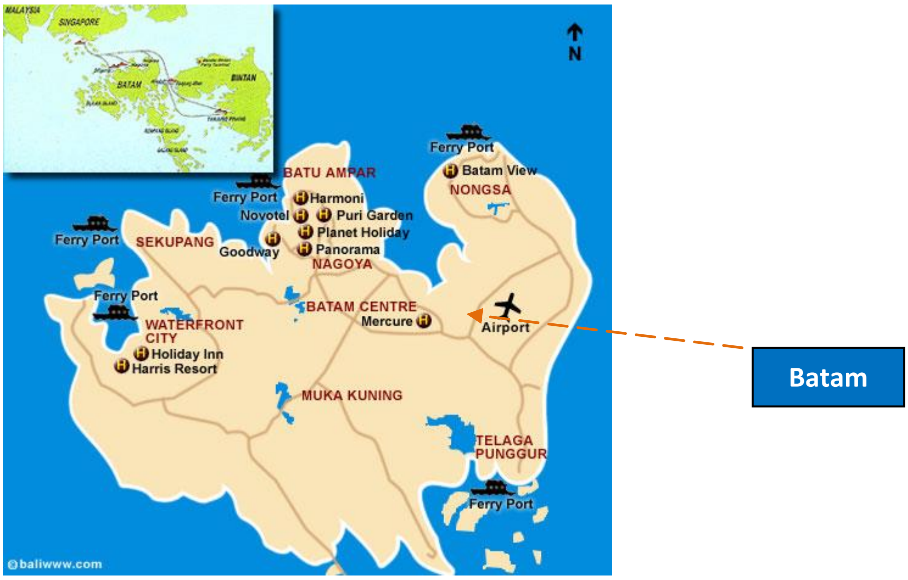
For HOTAC at Balikpapan and Banjarmasin cities - hotels as far as possible from the sea / estuary should be chosen, commensurate with availability. Staff should be accommodated higher than the fourth floor

For Balikpapan and Banjarmasin HOTAC and also for ground operating facilities at Balikpapan airport ***only*** - all staff to be briefed on tsunami risk and trained / drilled in recommended actions if 'caught in the open'

Target Date for Implementation - ASAP and by Hajj deployment date minus 1 month at latest

Note 1 - the above risk register item refers in the main to ‘people’. A similar risk register entry would have been additionally required for the potential threat to equipment, facilities etc. e.g. aircraft, ground equipment, operating facilities etc.

Note 2 - whilst the above example is predominately risk / threat based, it obviously has spin-offs for the business continuity aspects of the operation. For example, if a catastrophic tsunami were to hit Banjarmasin city but airline staff were not killed, injured, missing (possibly / probably due the safeguards put in place as per previous page) then the Banjarmasin operation would probably be able to continue (it will be noted from above that the risk to Banjarmasin airport from Tsunami is negligible - meaning that aircraft, supporting equipment and ground operating facilities will almost certainly be fully intact should an associated Tsunami risk actually be realised)



Figs 21A & 21B

SOUTH CHINA SEA
SULU SEA
0
100
200
KUDAT
KOTA BELUD
TUNKU ABDUL RAHMAN MARINE PARK
KOTA KINABALU
MT KINABALU
PORING
RANAU
TAMBUNAN
TURTLE ISLANDS
SANDAKAN
LABUAN
BEAUFORT
TENOM
MT TRUSMADI
SEPILOK
SUKAU
BRUNEI
BRUNEI
LAWAS
SABAH
LAHAD DATU
BORNEO RAINFOREST LODGE
BATU PUNGGUL
SEMPORNA
MIRI
NIAH CAVES
MT MULU
BARIO
TAWAU
SIPADAN ISLAND
BINTULU
TARAKAN
CELEBES SEA
SIBU
SARAWAK
SANTUBONG
KUCHING
SRI AMAN
BATANG AI RESORT
Balikpapan
PONTIANAK
KALIMANTAN
SAMARINDA
BALIKPAPAN
SELAT KARIMATA
MAKASSAR STRAIT
Banjarmasin
BANDJAMASIN
JAVA SEA

Summary Notes re *Risk* Management Procedure described above (in no particular order)

Risk Management Department / Business Unit

For the purposes of this guideline document (the one you are reading now) it is assumed that ***no*** such department / business unit exists within the organisation. Practically speaking this will probably mean that the person(s) appointed to manage ***BC matters*** within the organisation will also be assigned to look after the risk management aspects of same - and, consequently, this is also assumed in this guideline

What is contained herein ***regarding risk management*** is probably adequate for BC purposes from a ***theoretical*** aspect - and some persons with appropriate background, experience and skills will actually be able to turn the theory into practice and make a 'good job' of it

For the rest of us it is strongly recommended that appropriate external training is taken in the appropriate subject areas. Furthermore, it may be advantageous to engage an external expert to conduct the first ***risk*** management / assessment etc. - with the BC Manager 'understudying. Such expert should have appropriate ***aviation*** related experience

Training (Familiarisation)

It would be beneficial to provide some relatively brief and low-key training for * those persons (from the organisation) assigned to provide the information required in the 'risk assessment' elements of the 'understanding the organisation' task (e.g. identification of threats to specific activities; identification of subsequent consequences should threats be realised; estimations of likelihoods / probabilities of threats being realised; involvement in the eventual risk solution / control / treatment process etc.)

Such training, when combined with provision of a good quality risk management / assessment methodology document (written instructions on how to provide what is required) will be of significant overall benefit to the risk management / assessment process - and so is worth doing

* Specifically those persons (within and outside the organisation) most qualified and experienced so to do (i.e. subject matter experts). In general, the BC Manager, external consultant etc. is *unable* to provide what is required here

Risk Management (Assessment [Analysis]) - Outcomes

Outcomes from the risk management / assessment procedure (specifically within a ***business continuity*** related context) should have typically provided:

- A ***prioritised*** list of significant risks to the organisation (typically recorded in a document known as a 'Risks Register')
- Information necessary for implementation of risk management strategy and the associated (tactical) risk solutions / controls / treatments plan

- Identification of tactical solutions / treatments / controls (if any) **for which BC measures are most appropriate**
- Documentation related to all of the above
- Top management review and approval

* Consequence / Impact Categories

* See again related information pages 150 to 153

The term ‘consequence / impact categories’ refers to those key main and key supporting activities + their processes, procedures, inter-dependencies etc. (being directly and / or indirectly associated with delivery of an organisation’s key product / services / operations) - which, if affected (typically adversely) in some way as a result of a particular risk occurrence, might have a significant impact(s) on the ability of the organisation to deliver said key product / services / operations

Consequence / impact categories must be specific to the organisation ***and*** activity to which they are to apply

Examples of some generic consequence / impact categories include financial, operational effectiveness / efficiency, brand / image / reputation type issues, stakeholders (particularly customers / clients and shareholders), statutory / regulatory, injury / death etc. For aviation in particular we can add the categories of ‘aviation related safety’ and ‘aviation related security’

To ensure consistency within an (the same) organisation with regard to the closely associated subjects of ***risk*** probability assessment and ***business*** (continuity) impact assessment, a ***common*** or near common set of consequence / impact categories should be available and applied to ***BOTH*** processes

Note - do not confuse ‘risk’ with ‘consequence’s e.g. ‘injuries’, ‘financial loss’ and ‘reputation damage’ etc. - are not risks……………………..they are potential consequences of realised risk

Risk Management / Assessment - Review

Good practice means that risk management / assessment be reviewed at least annually - but also on an ‘as required’ basis in the event of:

- Major change(s) to strategic business objectives
- Significant change(s) in internal business processes, location, technology etc.
- Significant change in the external environment, such as regulatory, market, supply chain change
- In conjunction with any new BIA

The risk management / assessment process does not necessarily need to be repeated in its entirety at review i.e. only those key products / services (including associated processes, activities, resources, dependencies etc.) affected by significant risk and or BIA change need to be thoroughly reviewed. For evaluation / audit purposes, same may require periodic ‘sample’ review & confirmation of previous risk management / assessment

Extract from ISO 22313 / **OPERATIONS** / **Risk Assessment** - 8.2.3

*'……………………The organisation should select an appropriate method for identifying, analysing and evaluating **risks** that could lead to disruption. **ISO 31000** sets out the principles of risk management and associated guidelines. Typical elements which should be included in the context of ISO 31000 are:*

- ***Identification of Risks*** *- Potential sources of risk to the organisation's prioritised activities and the processes, systems, data, people, assets, suppliers and other resources that support them. These can come from:*
    - *Specific threats that could at some point disrupt activities and resources (e.g. fire, flood, power failure, staff loss, staff absenteeism, computer viruses, hardware failure)……………………. and*
    - *Disruptions, which could arise from vulnerabilities within resources (e.g. single points of failure, inadequacies in fire protection, lack of electrical resilience, inadequate staffing levels, poor IT security and resilience)*

- ***Analysis of Risks*** *- An understanding of the risk so that it can be evaluated and the most appropriate treatment (solutions) determined. This should involve:*
    - *Considering the causes & sources of risk, the likelihood of both positive & negative consequences & the effect that other factors could have on the likelihood*
    - *Determining the risks, based primarily on their likelihood & anticipated consequences + accounting for the effectiveness & efficiency of existing controls*

  A key parameter in the analysis is likelihood*, so confidence in its validity (based on divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling) should be considered and brought to the attention of decision makers and other interested parties. The analysis can be qualitative, semi-quantitative or quantitative*

- ***Evaluation of Risks*** *- An evaluation of which disruption-related risks require treatment. This should focus on the resources required by activities with high priority or with significant replacement lead time*

To review the author's (i.e. author and owner of this guideline document - the one you are now reading) thoughts on the undesirable situation whereby BC practitioners (particularly those with low experience; just starting out; low budget etc.) are now implicitly required to 'understand' (and thus also purchase or otherwise somehow procure) the ISO documents associated with '**risk assessment**' - see Note 6 / page 36 of *separate* (but related) guideline document CRPM Part 3 / Volume **1**

Section 5 / **2B** / **4**

Business Continuity Requirements - ***Resources Analysis***

The outline method of accomplishing this analysis has already been described in Section **5 / 2A**. More detailed information can be found in Section **5 / 3** / 5 (page 215)

The BIA analysis will actually capture much of this ‘resources related’ data if completed correctly and, practically speaking, the two analyses might be better merged into one

Organisations should be aware when determining such resource requirements that they can only be ***tentative*** at this point in the BCMS introduction task

They will need to be reviewed and adjusted (changes / deletions / additions etc.) if so required, during the ‘BC Strategy & Tactical Treatments / Solutions / Controls etc.’ selection process found later in this guideline document (starting pages 197 [abbreviated version] and 206 [full version])

Section 5 / **2B** / **5**

Understanding the Organisation - ***Summary***

- Appoint most appropriate person(s) to the task
- Re-confirm top management backing and support (including required resources)
- Account for stakeholders / other interested parties with regard to their interests in the organisation (and vice versa)
- Make all appropriate preparations for the task
- Conduct the task
- Analyse and assess the derived data
- Establish and document the outcomes
- Make a ‘first educated guess’ at the resources required to implement the appropriate outcomes
- Present everything to top management for approval and sign-off
- Go on to the next step which is ‘Formulating / Setting BC Strategy & Associated Solutions (treatments / controls)’

Some External References re Section 5 / 2 - **Understanding the Organisation**

For some further perspective on what has been written in Section 5 / 2 above (particularly re BIA and Risk Assessment) - appropriate sections of the documents / information (found by following each of the below links) *might* be found useful. Some of this info etc. is 'official' and some comes from commercial sources. Some provides reasonable detail whilst others provide just a simplistic overview

The user / reader will note the sad lack of BC related info in general and * ***aviation specific*** BC matters in particular. In contrast, there is a relative abundance of ***risk*** information in this area

* That is hopefully not a problem as you are reading possibly the best such reference source available right now (fully updated to reflect appropriate parts of ISO 22301:2019 / ISO 22313:2020)

Keep in mind that BC is a component part of (the overarching) Risk Management discipline / subject (even if knowing same might not prove to be very helpful in the search for good, comprehensive reference sources which reflect the 2019 and 2020 versions of ISOs 22301 and 22313 respectively):

Business Impact Analysis

'***Business Continuity Guidelines***'

https://aviationemergencyresponseplan.com/wp-content/uploads/BC-Guidelines-W-Oz-Govt-3rd-Edn-June-2015.pdf

Government of Western Australia - an excellent introduction to BC as related to public (government etc.) type organisations. Whilst not aviation related it provides good coverage of the basics. (When the webpage at the end of the above link opens, scroll down and select the information you wish to refer to [presumably 'BIA' but the whole document is worth studying] under 'Business Continuity Guidelines' [September 2019])

'***Business Impact Analysis** - **Example Template***'

https://safetyculture.com/checklists/business-impact-analysis/

Risk Management

'***Risk Management Guidelines***'

https://aviationemergencyresponseplan.com/wp-content/uploads/RM-Guidelines-W-Oz-Govt-3rd-Edn-Sep-2014.pdf

Government of Western Australia again - same as with its BC equivalent (see further above), a good introduction to Risk Management - but again, not directly aviation related. You should read the entire document (September 2019)

Finnair

https://company.finnair.com/en

When webpage click on 'Investor Relations' [see menu top of page] - then click on 'Governance' - then click on 'Risk Management'). A useful, concise explanation regarding how Finnair manages its Risk Management accountabilities

Lufthansa

https://investor-relations.lufthansagroup.com/fileadmin/downloads/en/financial-reports/annual-reports/LH-AR-2021-e.pdf

LH Annual Report 2021 - see pages 76 to 92 - 'Opportunities & Risk Report'

Enterprise Risks Management in the Airline Industry

https://bura.brunel.ac.uk/bitstream/2438/11087/1/FulltextThesis.pdf Thesis - May 2015

Airports (In General)

https://www.nap.edu/read/22744/chapter/4 Application of Enterprise Risk Management at Airports

Hong Kong International Airport

https://www.hongkongairport.com/en/airport-authority/publications/annual-interim-reports/annual2018 See the 'Risk Management' section

Business Continuity Reference Books / Documents etc. - General

'***Operational and Business Continuity Planning for Prolonged Airport Disruptions***'

For another useful document (***freely available*** 'on-line' to download) the USA's Transport Research Board (TRB) has produced (November 2013) a guideline document and software tool for ***airport*** BC Planning. This guideline has been sponsored by the US Federal Aviation Administration

The above is a useful resource for basic airport BC. However, note that it was based on a now superseded (discontinued) BC standard (BS 25999) i.e. not on ISO 22301 / ISO 22313. However, as the latter two standards had been originally based on BS 25999 - this guideline might remain useful - as yet another source of aviation related BC information. You will find this document (including instructions for how to download the tool) at:

http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_093.pdf

From the same source (TRB) a further 'synthesis' report (October 2016) is available entitled '*Continuity of Operations* Planning for Small Airports'

You will find this document at: http://www.trb.org/Publications/Blurbs/175144.aspx

BC Institute (BCI) - '***Good Practice Guidelines*** (GPG) 2018' (ISO 22301 / 22331 oriented)

An extract from this document's 'official' introduction reads as follows:

'……………………The GPG is a comprehensive and independent BC knowledge source written by 'real world BC experts'. The GPG considers not just what to do, but why, how and when……………………'

It is available free to BCI members or can be purchased (for around USD $40) from BCI at:

https://www.thebci.org/training-qualifications/good-practice-guidelines.html

However, as at 2022, a 'lite' version of the GPG 2018 was available, which could be freely downloaded provided an associated registration form was completed. Follow below link for more details:

https://www.thebci.org/resource/gpg-lite-2018-edition.html

DRI International - ***Professional Practices for Business Continuity*** (USA oriented)

An extract from this 2017 document's 'official' introduction reads as follows:

'…………………The Professional Practices are a body of knowledge designed to assist the entity in the development and implementation of a BCM program. Use of the Professional Practice framework can increase the likelihood that no significant gaps will be present in your program as well as increase the likelihood that the various parts of the program will work cohesively in an actual event……………….'

Simply register with DRII to obtain on-line access to this document ***free of charge***:

https://www.drii.org/crm/login.php?redirecturl=https://www.drii.org/certification/professionalprac.php

(When the above webpage opens - you will need to '***sign-up***' - which is easy to do. When latter completed you should then '***log-in***' and, once done, look under the 'RESOURCES' drop-down menu and select '***Professional Practices***')

Deliberately Blank

Section 5 / 3A - DO - DEVELOPING the BCMS / **Selection of BC Strategy & Solutions**

ISO 22313 / OPERATION / **Business Continuity Strategies** & Solutions etc. - 8.3

(Determining BC Strategy - ***Simplified*** Version [see Section 5 / 3B for **Full** version])

(Full version starts on page 206)

The starting point here is to understand what ‘strategies’ and ‘tactics’ actually are - when used in the BC context? That done, we can get on with related matters in this Section 5 / 3

IMPORTANT: Referring to the title above i.e. ‘***Business Continuity Strategies and Solutions***’ the words ‘***and solutions***’ were only added (by ISO) with the advent of the October 2019 version of ISO 22301 (same goes for the February 2020 version of ISO 22313)

The word ‘solutions’ used as per above should more correctly and clearly be interpreted as ***tactics*** or, pedantically, ***tactical solutions to how an associated BC strategy might be achieved***

It is strongly recommended that the serious reader now reviews the definitions of ‘Business Continuity Strategy’ and ‘Business Continuity (Tactical) Treatments / Solutions / Controls etc.’ (found in separate [but related] document CRPM Part 3 / Volume 1)

Strategy specifies an organisation’s (or a person’s) longer-term / higher level goals, mission, objectives etc. - typically expressed in ***general*** terms only

General Tactics drill down (to a pre-specified level) to the actual means of how an ***associated*** strategy might typically be best achieved / accomplished etc. i.e. the ***detail in general***

Operational Tactics drill down even further i.e. the detail ***specifically***

In this guideline document (the one you are reading now) ‘General’ and ‘Operational’ Tactics are ***jointly*** expressed by the single term ‘**BC Tactical Treatments** / Solutions / Controls etc’

Those requiring a more in-depth explanation of strategy and tactics (in the general sense) are referred to the excellent (brief) article found by following the below link:

https://www.clearpointstrategy.com/strategy-vs-tactics/

What does ‘Selection of BC Strategy & Solutions’ mean in ‘plain’ language?

The following information attempts to ‘simplify’ the meaning, purpose, practical application etc. of the ISO 22313 term (clause 8.3.3) *‘Selection of BC Strategy & Solutions’*. This is required as full and correct completion of this task (following on from the ‘understanding the organisation’ task) is fundamental to the reason for introducing a BCMS into an organisation

Furthermore (as already mentioned previously & frequently) much of the reference material in ISO 22313, ISO / TS 22331 et al ……… is not as clear / helpful / comprehensive etc. as it might be, particularly re this (business continuity strategy, tactics [solutions] etc.) section

Recap

Up to this point in the BCMS implementation (**DO**) task we have (amongst lots of other things) identified and / or predicted and / or conducted and / or produced etc. an organisation's:

- **BCMS Objectives, Policy and Scope** (BC Requirements)
- **STAKEHOLDER** (+ other Interested persons) *Analysis*
- **BUSINESS IMPACT** *Analysis* (BIA)
- **RISK MANAGEMENT** *Analysis* (*Assessment)* (RA)
- *(BC Requirements)* - **RESOURCES** *Analysis*

Understanding the Organisation

- **RESULTING / CONSEQUENTIAL LEVELS of OVERALL RISK** to the subject(s) under consideration (latter typically being an organisation's key [prioritised] products / services / activities / operations etc.)
- **TARGET TIMESCALES** *(**MTPD** & **RTO**)* within which pre-specified target levels of key [prioritised] product / service etc. resumption *(**MBCO**)* should be achieved, following a significant disruption type event

Consequently, we have been able to choose *(as **just one** of the several '**RISK** treatments' available - and if appropriate)* to:

'…………. **Reduce** the **impacts** of realised risk i.e. plan to manage / control / treat etc. the risk ***AFTER*** it has actually occurred, by use of ***BC** measures* etc. ………….'

The words *('by use of BC measures')* above can be replaced, (with [almost] exactly the same meaning) by the words *'by selecting and using the appropriate **BC Strategies & Solutions**'* - it's (almost) as simple as that!

IMPORTANT - the choice of '**BC** measures (strategies) available' is based ***initially*** on a high level (strategic / big picture) view - hence use of the word '*strategy*' in the term 'BC strategy'! The actual application (hands on use) of any particular strategy is known herein as applying associated '***BC Tactical Treatments*** / *Solutions* / *Controls etc.*' (i.e. strategies transform into tactics)

The who, what, when, where, why and how re actual application of BC Tactical Treatments etc. - should be explained and documented etc. in associated '***BC Plans***'

An associated BC '***system / structure***' is required to 'manage / control / operate' all of the above. ISO uses the misleading term '*Incident Response Structure*' for this. In contrast we use herein the term '***Disruption Support Units***' (see definitions in separate [but related] document CRPM Part 3 / Vol 1)

All above needs to be ***resourced***, ***trained***, ***exercised***, ***maintained, reviewed*** and ***continually improved***

To summarise, BC strategies are typically ***higher level*** categorisations used by an organisation to better produce, manage, facilitate etc. its in-scope business continuity requirements (policy, objectives, plans, structures, resources etc.) Very simplistically speaking, there are just 3 such 'higher level' categorisations:

- ***Full***, **24H** key (prioritised) product / service / operation / activity / process etc. **availability** - i.e. the activity etc. **must** be capable of (almost) immediate, full resumption (continuation) following a significant disruption event……………………AND / OR

- ***Resumption*** of the key (prioritised) product / service / operation / activity / process etc. is required - ***within pre-agreed MTPDs*** / ***RTOs*** - to ***pre-agreed minimum operating levels*** (***MBCOs***) i.e. scaling down on continuation of specific activities, procedures etc. - within specified timescales and levels of operation, following a significant disruption event……………………AND / OR

- ***Do nothing*** i.e. product / service / operation / activity, processes etc. which (from a business continuity viewpoint) can be suspended / deferred etc. for an appropriate time period. The detail will be clarified in the associated RTOs (e.g. RTOs such as 'Indefinite'; '6 months' etc. are typically associated with a 'do nothing' strategy) and additional, explanatory material

Confusingly, ISO 22313 of 20***12*** had 'mixed-up' BC ***strategy*** with the associated but subordinate ***tactical*** measures (BC tactical treatments / solutions / controls etc.) required in order to implement / carry out said strategy / strategies. ISO 22313 of 20***20*** had not improved matters significantly - but had at least tried by stating:

> *'………………A BC **strategy** should comprise at least one BC tactical '**solution**' but more may (almost certainly will for larger / more complex organisations) be required. Said BC tactical **solutions** include approaches, arrangements, methods, procedures, treatments, actions etc. - necessary to implement associated BC strategy / strategies……………………'*

Application of BC strategies and associated 'solutions' (i.e. associated '***BC Tactical Treatments*** / *Solutions* / *Controls*' for the latter) + associated plans, response structures etc. can enable organisations to resume disrupted operations / services etc. within stipulated time frames at pre-defined (but not full) levels. The identification, selection, use etc. of same are based on the outcomes of the 'understanding the organisation' task; consideration of associated cost / benefit factors etc.

Associated procedures necessary to identify / select BC strategies and associated tactical solutions (i.e. associated '***BC Tactical Treatments*** / *Solutions* / *Controls*' for the latter) etc. are required, including review and approval. Options should consider strategies / solutions etc. which can be implemented * before and / or during and / or after a disruption. (Note: * Pedantically speaking 'actions taken ***before*** a potential disruptive event' occurs relate to elements of ***risk management*** other than [i.e. NOT] ***business continuity***)

In summary, ***BC strategy*** provides the higher level ***framework*** for deciding the ***actions*** etc. necessary to re-establish continuity (of key [prioritised] product / service /operation / activity / process etc.) following significant disruption of same. Within that framework***, BC tactical treatments etc***. actually ***decide*** and ***define*** those actions in sufficient detail - such that they may be further expanded upon and implemented / executed operationally 'on the day'

The latter is facilitated via preparation of associated BC ***Plans*** & ***Procedures*** (documentation) and by employing the structure and manpower resources of e.g. a '***BC* * *Incident Response Team***' (latter team known in ***this*** guideline document as '***Disruption Support Units*** - **DSU**) etc.

* '***INCIDENT RESPONSE TEAM***' (IRT) is an ISO 22301 / 22313 term. **As its use in *aviation related* contingency response planning** (including BC planning) **is potentially confusing** (see the associated 'Glossary' definitions in separate [but related] document CRPM Part 3 / Vol 1 for why this is so) we use the term '***DISRUPTION SUPPORT UNITS***' herein instead (See also ***this*** document pages 100 to 104)

Just as BIA and RA are inextricably linked, so are BC Strategy and BC Tactical Treatments / Solution / Controls etc. In fact, differentiation between the latter two is almost (but not quite) academic, when used in the ***BC*** context

A further consideration is made within the BC Strategy framework - and that is the ***final*** identification, co-opting (e.g. for people), adaptation (of appropriate, existing equipment, facilities, technology etc.), procurement (e.g. for additional equipment, facilities, technology etc.) and costing (budget etc.) of the ***resources*** necessary to 'make it all work' in practice

But before moving on let's clarify an extract from ISO 22313, Clause 8.3.2.1 ('Identification of Strategies & Solutions - General'). The text of interest is reproduced just below:

'………………The organisation should identify appropriate strategies & solutions for:

- Protecting prioritised activities
- Stabilising, continuing, resuming and recovering prioritised activities
- Mitigating, responding to and managing impacts ………………'

The first bullet point above is a '*Risk Management*' measure (i.e. ***not pedantically*** a ***BC*** measure) - thus is outside the scope of this guideline document and BC in general. The second bullet point may be simply summarised as 'by using ***Business Continuity*** measures'. The third bullet relates to **both** *Risk Management* and *Business Continuity*. As the document you are reading now only concerns BC, it should be interpreted and applied as such accordingly

ISO 22313 unnecessarily devotes almost 2 pages to the above. It also cross-refers the reader to (separate document which you need to buy) ISO / TS 22331. Don't waste your time and money on the latter (for reasons, see [separate but related document] CRPM Part 3 / Vol 1 / page 34)

The 8 Steps of BC Strategy Implementation (**SIMPLIFIED** *Version*)

Research / decide which particular '**BC measures**' (i.e. ***BC strategies*** **+** their associated, subordinate ***BC tactical*** treatments / solutions etc. **+** the identification and co-opting / adapting / costing / procuring etc. of the associated ***BC resources*** required [to make everything work as required] etc.) might be most appropriate to the anticipated level of adverse ***impact***(s) - which any particular (realised) ***threat***(s) might pose on any particular (organisation's key [prioritised] products / services / operations etc. related) activity, process, resource etc. (such 'impacts', 'threats', 'risk' etc. being outputs of the '***understanding the organisation***' task)

The task immediately above can simply be re-worded (in ISO 22313 terminology) as ***'determining** (working out)* ***BC Strateg**y & **Solutions**'*. A more detailed 'explanation might be:

- Work out which ***BC strategies*** meet the ***BC Policy***, ***Objectives*** & other organisational ***BC requirements*** (including consideration of *RTOs* / *MBCOs* / *other appropriate considerations* [as they relate to specific key (prioritised) activities, processes, resources etc.] - obtained from outputs of the '***understanding the organisation***' task)

- Re-confirm and / or adjust already calculated ***RTOs*** and ***MBCOs*** (as required) as a consequence of completing the bullet point step immediately above

- As part of any particular strategy, select the most appropriate ***'BC tactical treatment / solution*** *etc.'* response(s) (based on what it is [specific activity, process etc.] such responses are potentially / actually to be 'applied' to) from available options

- Work out, consolidate, cost, budget and (subject to costs / benefits analysis) procure the ***resources*** required to meet the strategies and associated tactical treatments / solutions etc. provisionally and / or finally chosen, as per the above ………………'

The above is accomplished (simplified version) via the following steps:

Step 1 - Choose ***Provisional*** BC **Strategies**

As already mentioned, there are three basic choices:

- ***Full***, **24H** key (prioritised) product / service / operation / activity / process etc. **availability** - i.e. the activity etc. **must** be capable of (almost) immediate, full resumption (continuation) following a significant disruption event……………………AND / OR

- ***Resumption*** of the key (prioritised) product / service / operation / activity / process etc. is required - ***within pre-agreed MTPDs*** / ***RTOs*** - to ***pre-agreed minimum operating levels*** (***MBCOs***) i.e. scaling down on continuation of specific activities, procedures etc. - within specified timescales and levels of operation, following a significant disruption event……………………AND / OR

- ***Do nothing*** i.e. product / service / operation / activity, processes etc. which (from a business continuity viewpoint) can be suspended / deferred etc. for an appropriate time period. The detail will be clarified in the associated RTOs (e.g. RTOs such as 'Indefinite'; '6 months' etc. are typically associated with a 'do nothing' strategy) and additional, explanatory material

Each potential BC strategy (as it relates to a specific activity, process etc.) is evaluated for advantages and disadvantages - and the most appropriate ***tentatively*** chosen. Based on this choice, RTOs and MBCOs already assigned during the BIA may be confirmed and / or adjusted

In tentatively choosing the appropriate strategies, initial consideration must be given to the estimated * implementation costs (typically via a ***costs*** / ***benefits analysis***) and also to the 'knock-on' consequences of inaction and / or inadequate action

* Note - costs are looked at again in more detail once the provisional tactical treatments / solutions etc. and supporting resources have been identified - see 'Step 4' further below

Step 2 - Choose ***Provisional*** BC (Tactical) **Treatments** / Solutions / Controls etc.

Having now selected a provisional BC strategy as per above (other than the 'do nothing' option) - we drill down / expand further (i.e. become more 'hands on' / 'tactical') within that strategy, in order to ***further*** tentatively ***identify*** specific, appropriate and adequate additional measures to take - in order to ***facilitate the selected strategy to actually be accomplished / able to happen / work in reality*** - when needed

The reader will by now be aware that such 'specific, appropriate and adequate additional measures' are known herein as '**BC** (tactical) '**Treatments** / Solutions / Controls' - of which there is a relatively wide choice. However, the selection and use of the most appropriate BC tactical treatment 'choice / choices' (there is typically more than one) is what is important (as will be seen later)

The above tasks (selecting provisional BC strategy and associated BC tactical treatments etc.) are repeated for every one of the organisation's (key [prioritised] products / services / operations etc. related) activities, processes, procedures etc. - previously identified and listed as needing such during the 'Understanding the Organisation' task

Reminder: '**BC Tactical Treatments**' are simply a sub-division / drill-down of 'BC Strategy'

Note: Of course, the decision can be made, with appropriate justification(s) (e.g. as based on the declared and documented '**risk appetite**' of the organisation) to potentially choose the '**do nothing**' strategy (the third bullet point strategy already referred to in 'Step 1' on the previous page)

This latter strategy is typically selected following a ***cost*** / ***benefits analysis*** of the associated BC tactical treatments / solutions etc. available - where the potential benefits of using an appropriate, specific treatment(s) etc. are (or are estimated to be) outweighed by the costs (whatever the term 'costs' might be referring to in such circumstances - it need not be 'financial') of implementing such treatment(s)

There may be potential adverse implications in choosing the 'do nothing' strategy - if not managed correctly. Such implications typically affect brand, image and reputation issues; financial matters etc.
Accordingly, in choosing this particular strategy it is important to identify any further potential, (knock-on) adverse impacts which might arise consequentially ***as a result of doing nothing*** - and ***pre***-establish appropriate (additional) counter-measures accordingly

For example, the need to communicate effectively with stakeholders / other interested parties as to 'why the decision to do nothing' was taken; e.g. providing some form of compensation or similar to those disadvantaged (such as airline passengers prevented from flying) as a result of 'doing nothing' etc.

Furthermore, in situations where RTOs might be measured e.g. in months or even longer, waiting (doing nothing) until after the incident is over to decide on a strategy to resume / recover the associated (disrupted) activity, process etc. may be acceptable, particularly if the delivery of same does not require any specialist equipment, facilities or skills which might be expensive and/or difficult to obtain / acquire

Step 3 - Complete the 'Establish **Resource Requirements** (Analysis)' Task

This step is targeted at identifying, documenting and costing all of the potential ***resources*** which should be provided (in support of the provisional BC strategies and associated tactical treatments etc. chosen as per steps 1 and 2 above and [+] what follows thereafter) - in order to deliver a consolidated view of such resource provision

This analysis is also used to assist in:

- Identifying and simplifying unnecessary (resource related) complexities
- Identifying and correcting conflictions (e.g. so that different activities, processes etc. are not planned to concurrently use the same resource(s) for business / operational etc. resumption - unless feasible and desirable so to do)
- Identifying / implementing areas of resource provision which can beneficially be consolidated e.g. where the ***same*** BC strategy & associated tactical treatment(s) etc. might concurrently meet the BC requirements of several different activities, processes etc.
- Looking at opportunities for 'enabling purchasing leverage' (e.g. financial discount) when procuring the appropriate resources from external (third party) sources
- Validating that proposed BC strategies and associated tactical treatments etc. are in line with associated BC Policy, Objectives, Scope and Risk Appetite etc.
- Eventually establishing more definitive (resources associated) info and costs in relation to the ***entire*** process of introducing a BCMS into the organisation

Important - The subject of ***resources*** deserves particular attention. It is suggested that those responsible for introducing BCMS into an organisation pay particular attention to the ***RCA*** (* Resources Consolidation Analysis) and other appropriate 'resources' related requirements - particularly if the intention is to ***certify*** a BCMS to BC Standard ISO **22301** ....or ***formally align*** a BCMS with ISO **22313**

* See Section 5 / 3.5 starting page 215

The resource requirements as per ISO 22313 / clause **8.3.4** cover (at a higher level overview):

- People (including 'Partners' & other 'Interested Parties'
- Information & Data etc.
- Buildings / Work Environment - and associated Facilities, Utilities etc.
- Equipment / consumables etc.
- ICT Systems etc.
- Transportation / Distribution / Logistics etc.
- Finance / Budget etc.
- Suppliers / Supply Chain etc.

Reminder: The '**RCA**' is simply a sub-division / drill-down of 'BC Strategy'

For cross reference purposes, the subject of *BC **resources*** also appears herein at:

Section 4 / **1** / 3 of this guideline (page 67) - based on:

ISO 22313 / 5.1 to 5.3 - **LEADERSHIP & COMMITMENT**

Section 4 / 2 of this guideline (page 95) - based on:

ISO 22313 / 7.1 - '**SUPPORT** / Resources'

Section 5 / 2 of this guideline (pages 135 & 192) - based on:

ISO 22313 / 8.2.2 - **OPERATIONS** / BIA

Section 5 / 3.5 of this guideline (page 215) - based on:

ISO 22313 / 8.3.4 - **OPS** / BC Strategy & Solutions - Resource Requirements

Note 1: The subject of 'resources' gets a significant number of ***additional*** 'mentions' throughout the whole of (ISO 22313) - ***Clause 8***. These 'mentions' should all be noted and, where appropriate (e.g. if it is an organisation's intention to ***certify*** to the requirements of ISO 22301) acted upon as required. Access to the (latest versions) ISO 22301 and 22313 standards would be necessary for this to be accomplished. However, what is referred herein (i.e. in the document now being read) - on the subject of 'resources' - should be sufficient for those organisations wishing to ***align*** (i.e. ***not*** 'certify') with ISOs 22301 / 22313

Note 2: - there is significant overlap in the resources related info provided in ISO 22313. Little effort seems to have been made (by the ISO Technical Committee which produced it) to better manage / mitigate same (which may thus be potential sources of confusion to some users / readers)

Step 4 - Assess / Review BC Strategy etc. **Implementation Costs** - (Costs / Benefits Analysis)

- Estimate costs of implementing & maintaining continuity (BC Tactical Treatments etc.) for the chosen BC strategy / strategies (using the info from 'step 3' above + any other considerations [financial and equivalent] to be accounted for)

- Validate (or not) that said BC strategies etc. reflect the amount and / or type of business / activity etc. 'at risk' e.g. a million dollar BC strategy would be inappropriate when related to protecting $100,000 worth of 'whatever'- whereas the same strategy might be appropriate where e.g. danger of death or serious injury are considerations

- Where cost is ***not*** commensurate with benefit - an associated review of the proposed strategy / treatment(s) etc. is required

Reminder: '**Review of BC Strategy Costs**' is simply a sub-division / drill-down of 'BC Strategy'

Step 5 - BC related **Communications** with Stakeholders / Other Interested Parties

Research, decide / agree and document the organisation's ***BC communications*** '***sub***-strategy' - set against the background of the most likely 'worst case' BC disruption scenarios which could impact on the organisation - particularly those having adverse implications re stakeholders / other interested parties (the outcomes of the 'understanding the organisation' task will be useful here).

Reminder: '**BC Comms**' sub-strategy is simply a sub-division / drill-down of 'BC Strategy'

Step 6 - Work **Backlogs**

Decide and document the organisation's ***sub***-strategy for dealing with disruption related work backlogs

Reminder: '**Work Backlog**' sub-strategy is simply a sub-division / drill-down of 'BC Strategy'

Step 7 - Dealing with Activities, Procedures etc. ***not*** initially assessed as being critically time-sensitive (prioritised) or 'critical' (prioritised) in any other sense

Decide and document the organisation's ***sub***-strategy for reviewing and dealing with 'Understanding the Organisation' identified activities, procedures, resources etc. - which were ***not*** prioritised (for attention) during same for 'BC related action' purposes, but which were nevertheless still thought worthy of re-consideration from a BC viewpoint - 'at some later time'

Reminder: Dealing with '**Non-critical Issues**' is simply a sub-division/drill-down of 'BC Strategy'

Step 8 - **Approval**

In conjunction with the outcomes of 'Steps 1 to 7' above - recommend the finally chosen 'BC Strategies' and their 'BC Tactical Treatments / Solutions etc.' (together with estimated costings and any other appropriate information) to Top Management for approval and (hopefully) clearance to proceed further with the BCMS project

Reminder *- for simplicity,* ***only*** *MTPD & RTO have been considered in this guideline document. However, when / if planning BC strategy for recovery of* ***information and data type assets***, ***MTDL*** *&* ***RPO*** *will additionally apply - and* **MUST** *be accounted for accordingly*

Starting next page - we shall look at the above steps again - but in a little more detail

Section 5 / **3B** - **DO** - DEVELOPING the BCMS

Determining BC Strategy and Associated Tactical Treatments / Solutions

ISO 22313 / OPERATION / **Business Continuity Strategy and Solutions** - 8.3

FORMAL Version (see Section 5 / 3A for ***simplified*** version)

Section 5 / 3B / **1** - Background

Assumption

Moving forward, it is now assumed that the user / reader has read and understood what has been written in Section 5 / 3A

Recommendation

It ***may*** be found useful to consider ***differing scenarios*** (and their potentially adverse impacts on the organisation) - when developing ***BC strategies*** and their associated ***tactical treatments*** / solutions etc. Note that the underlying ‘causes’ of the scenarios are irrelevant for the specific purposes used here - but in reality ***will*** require consideration, and, as required, appropriate action to remove, avoid, mitigate etc. (insofar as is possible / practicable / feasible / desired / mandated etc.)

Some ***typical*** scenarios for consideration (which will require ‘mixing & matching’ to the organisation’s actual [real life] circumstances) ***might*** include (list is ***not*** exhaustive):

- Safety related crisis (e.g. * catastrophic aircraft accident; unsafe ATC procedures etc.)
  * As a consequence, the accident airline’s main operating airport is closed for a week
- Security related crisis (e.g. hijack / unlawful interference, credible bomb warning etc.)
- Statutory / regulatory related crisis (e.g. major, longer term regulatory breach)
- Brand / image / reputation related crisis (e.g. an ‘airline’ has been falsifying its aircraft maintenance records with top management knowledge)
- Financial crisis (e.g. recession; cyclical downturn in aviation market; competition etc.)
- Deterioration of product / service quality etc.
- Deterioration of operational performance
- Unavailability of premises, facilities, plant etc. (e.g. due fire / flood; terrorist act etc.)
- Lack of resources - including people (e.g. power failure, industrial action, pandemic)
- Failure or lack of technology (especially ICT)
- Failure or reduced performance of a key supplier, partner etc. (e.g. industrial action)
- Transportation / distribution crisis (unavailability of fuel)
- Environmental crisis (e.g. volcanic ash; hurricane; earthquake; tsunami; bush fires etc.)
- Public Health crisis (e.g. epidemic; pandemic)
- Staff and / or public wellbeing related crisis (e.g. terrorism or pandemic again)

Such scenarios will also be of use later (Sub-section 5 / 4) when preparing ***BC** (Response) **Plans***

Reminder

With regards to the outputs of the 'understanding the organisation' task (Sub-section 5 / 2 herein) - the organisation is now ready to research, determine, select, gain TM approval for implementation etc. - the most appropriate BC Strategies & their associated BC Tactical Treatments / Solutions etc. - as related to the organisation's actual, operating circumstances

The associated resource requirements and provisional approval of associated costings / finance / budget etc. for same also needs to be researched, determined, reconciled, provisionally approved - and made ready for procurement, implementation / application etc.

Where possible and advantageous so to do, consolidation opportunities / possibilities re all of the above should also be researched, identified and implemented

*ISO 22313:2020 - clauses **8.3.1** to **8.3.4***

Clauses 8.3.1 to 8.3.2.4 have already been addressed in the boxed information shown on page 200 (of the document which you are reading now)

Re Clause 8.3.3 (Selection of [BC] Strategies and Solutions) see Section 5 / 3B / 3 (starts bottom of next page) together with Section 5 / 3B / 4 (starts page 209) for further details. Both are part of the document which you are reading now

Re Clause 8.3.4 (Resource Requirements) see Section 5 / 3B / 5 (starts page 215) of the document which you are reading now

Rest of this Page is Deliberately Blank

5 / 3B / **2** - General

__Reminder__ - for simplicity, only __MTPD__ & __RTO__ have been considered in __this__ guideline document. However, when / if planning BC strategy for recovery of __information__ and __dat__a type assets, __MTDL__ & __RPO__ will additionally apply - and __must__ be accounted for accordingly

Adequate completion of the tasks / requirements specified in this sub-section 5 / 3B should ensure that the determination and selection of ***BC strategy*** (along with everything else which follows on e.g. choices of associated ***BC Tactical Treatments*** / Solutions etc.; e.g. provisional identification and costing of associated ***resources***; e.g. production of associated ***BC Plans*** etc.) within the organisation adequately supports delivery of its key services / products / operations - via the latters' associated key (prioritised) activities, processes, resources, dependencies etc.

Note - the organisation should ***evaluate*** the ***provisional*** BC strategy (along with everything else which follows on etc.) to determine if such choices and their associated BC tactical treatments / solutions etc. might themselves introduce ***new risks*** which, (obviously) not having been considered in the 'understanding the organisation' task, might subsequently (now) require such consideration

Documentation of a finalised BC strategy (along with everything else which follows on) + 'sign-off' approval by the organisation's top management, is the target here. When this has been accomplished the BC strategy should be:

- Actively disseminated throughout the appropriate parts of the organisation
- Accounted for in appropriate, associated BC documentation (e.g. BC plans - see sub-section **5** / **4**)
- Actively referenced, explained etc. during BC training, exercising etc.
- Provided / explained etc. to appropriate (specifically selected by the organisation) stakeholders / other interested parties

If the above is done effectively, efficiently & comprehensively - not only will the BC strategy serve as a top level reference for the ***remainder*** of the BC implementation programme (including choices of specific, associated BC tactical treatments / solutions etc.; production of associated BC plans & procedures; set-up, equipping, manning and operation of an associated, appropriate response structure etc.) but it can also be used to keep any ***actual*** BC response approximately on course, despite the various conflicting & confusing ***tactical*** parameters which will typically be evident in such circumstances - 'on the day'

5 / 3B / **3** - Selecting BC Strategy

The above has already been adequately described in Sub-section 5 / 3A - **Step 1** (pages 197 to 201). Whilst this is an important task, it is relatively simple to perform and is thus not described further here, except for what follows at the top of the next page:

Note - if there are any ***existing*** BC strategies ***already*** in place - review same (i.e. by conducting a 'Gap Analysis') and assess suitability for retention, adjustment, abandonment etc.

Review of BC Strategy

A review of active BC strategies should be carried out after any continuity capability has been tested (i.e. in an exercise or for real) - and / or at least once a year and / or following similar reviews of the component parts of the 'understanding the organisation' process (BIA, RA etc.)

A ***significant change*** in any of the following should also prompt a similar review:

- Major change(s) to strategic business objectives
- Significant change(s) in internal business processes, location(s), technology etc.
- Significant change in external environment e.g. regulatory, market, supply-chain etc.

An appropriate ***maintenance*** policy should be established to ensure that active BC strategies remain relevant, accurate, current, complete, adequately documented etc.

5 / 3B / **4** - Selecting, Implementing & Managing 'BC ***Tactical*** Treatments / Solutions etc'

This sub-section requires the investigation, selection, approval, documentation, introduction and 'management' of the appropriate ***BC tactical*** measures (BC Tactical Treatments / Solutions etc.) considered necessary to ensure continuity of operation (as related to a specific / associated / 'parent' BC strategy) during / following a significant disruption event impacting on the organisation

The chosen BC tactical treatments etc. are directly related to the associated key activities, processes etc. (designated for such treatments) as per the outcomes of the '***understanding the organisation***' and '***selection of BC strategy***' tasks

Appropriate BC tactical treatments etc. are chosen so that they:

- Meet the requirements of the associated (parent) BC strategy
- Are 'appropriate' to the organisation (size, complexity, location, methods of doing business, etc.)
- Are capable of consolidation (where possible & advantageous so to do)
- Meet declared budgetary, resources and other constraints
- Are in line with the organisation's declared and current 'risk appetite'

The generic ***scope*** and ***choices*** of BC tactical treatments etc. are typically related, in one way or another, to (single and / or combined) uses of the following ***resources***: (ISO 22313 - [8.3.4] refers):

- People (Having acquired / retained / maintained the necessary BC associated skills, experience, knowledge etc. - 8.3.4.2.1)
- People (To man / operate 'Disruption Support Units [latter is the BC related element of an overarching 'Incident Response Structure']' - 8.3.4.2.2)

- People (To Resume Activities - 8.3.4.2.3)
- Information & Data (hard copy and electronic [soft copy] - 8.3.4.3)
- Buildings (premises / facilities), Workplaces & Associated Utilities (- 8.3.4.4)
- Equipment (including Plant), Consumables etc. (Core supplies / goods / stock / machinery / tools etc. - 8.3.4.5)
- Technology (predominately ICT and associated 'systems' - 8.3.4.6)
- Transportation and Logistics (8.3.4.7)
- Finance (8.3.4.8)
- * Partners (8.3.4.9)
- Suppliers / Supply Chain (8.3.4.9)
- Other appropriate Stakeholders / Interested Parties (not already included above)
- Emergency Services (typically provided & funded by national / local government etc.)
- Any other appropriate resources (not already included above)

* ISO 22313 (2020) refers to '***Partners***' (together with '***Supply Chain***') in its clause 8.3.4.9 but, in the body of said clause, explains matters re 'Suppliers' etc. but effectively does not cover 'Partners'. This is a serious omission e.g. airlines 'partner' with many organisations (not being suppliers etc.) to e.g. increase profit, provide better customer service etc.

Code-share ***airline*** services provide an example of the latter - where it is imperative that an associated assurance and evaluation etc. programme of same is in place and working as required. A similar example for ***airports*** might be commercial outlet partners (e.g. duty-free and other products etc.) at the airport - not being owned / operated by the airport itself

The task now is to:

- Identify the ***available*** **BC tactical treatments** / solutions etc. (falling within the scope of an associated BC strategy / ies) as specifically appropriate to ***each*** designated activity, process etc. outlined in the outcomes of the '***understanding the organisation***' task

- Provide inputs to identify the ***costs / difficulties / complexities*** etc. re ***resourcing, implementing and maintaining*** such **BC tactical treatments** / solutions etc.

- ***Provisionally select the most appropriate*** **BC tactical treatments** / solutions etc. for intended actual use - and

- Confirm that the provisionally selected **BC tactical treatments** / solutions etc. (provided associated resources would seem to be available, adequate and cost effective at this point) will ***meet the BC requirements as related to declared MTPDs, RTOs*** *and* ***MBCOs***

Note - ***if*** there are any BC tactical treatments / solutions etc. ***already*** in place - review same (by conducting a 'Gap Analysis') and assess suitability for retention, adjustment or abandonment

Outcomes from the above should include:

- A set of BC tactical treatments etc. * ***provisionally*** agreed to and approved by TM

* **Note**: - ***final*** approval should be provided ***after*** completion of the 'establishing resource requirements' task (sub-section 5 / 3 / **5**) and cost / benefit analysis (sub-section 5 / 3 / **6**)

- TM agreement and approval ** *in principle* - for the funding and resource acquisition necessary to eventually implement the provisionally agreed BC tactical treatments etc.

  ** **Note**: - ***final*** approval should be provided ***after*** completion of the 'establishing resource requirements' task (sub-section 5 / 3 / **5**) and cost / benefit analysis (sub-section 5 / 3 / **6**)

- A provisional list of the proposed tasks (sub-projects) required to implement (put in place) the agreed BC tactical treatments etc. - together with a provisional list of personnel / staff assignments for undertaking such tasks

  Note: - it may be necessary to ***re-appraise the 'parent' BC Strategy*** - should the associated and most appropriate BC tactical treatment / solution etc. choices prove unavailable or too costly. Additionally, where the ***only*** tactical treatments etc. available prove to be too costly, the affected product(s), service(s), operation(s), key activity (activities), process (processes) etc. may be nominated instead as ***exclusions*** from the BCMS scope (ISO 22313 - Clause 4.3.3)

  Where the organisation estimates that a particular ***threat***(s) is 'extremely unlikely' to be realised and / or the cost of protecting a key activity, procedure etc. will be too expensive - it may choose instead to accept the associated ***risk*** and periodically review this situation as part of its on-going BCMS ***performance evaluation*** (as per ISO 22313 - Clause 9)

Some Examples of Typical 'BC Tactical Treatments / Solutions etc.' - as per ISO 22313

Generic BC tactical treatments / solutions etc. [as per ISO 22313:2020 clause 8.3.2.3 / sub-paras 'a)' to 'd)'] typically include - (below list is far from being exhaustive):

- **Activity** relocation (e.g. providing additional manufacturing capacity elsewhere)
- **Resources** relocation and / or reallocation (including people) and / or replacement (e.g. establishing a 'work from home' [remote working] capability for key staff)
- Establishment of **alternative processes** (+ associated procedures etc.)
- Creation of **spare capacity**
- Augmentation of **skills** (e.g. via cross-training)
- Temporary **workarounds** (e.g. replace automated processes with manual alternatives)

IMPORTANT NOTE: Re ISO 22313 / clause 8.3.2.3 / Page 27 / Paragraphs a), b), c), and d) - following the words '........***Business continuity strategies may include the following***: ....' etc.

The above reference to '***Business continuity strategies***' should be interpreted in this guidelines document (the one you are now reading) as ***also*** including '***BC Tactical Treatments*** / *Solutions* etc.'

Looking at the boxed info on page 197 (of this guideline document).......... paras a), b), c), and d) (referred to just above) are classified herein as '***General*** **Tactics** (Solutions etc.)'. Drilling down further in the ***application*** of such general tactics, we would then be applying '***Operational*** **Tactics** (Solutions etc.)'.

Below that might come e.g. ***Plans***, ***Processes***, ***Procedures***, associated ***Documentation*** - and so on

Some Examples of Typical 'BC Tactical Treatments / Solutions etc. - *NOT* from ISO sources (1)

DRI International

Disaster Recovery Institute International (DRII) is a USA headquartered organisation. It describes itself as the 'oldest and largest non-profit entity' which helps organisations worldwide to prepare for and recover from disasters - by providing education, accreditation and thought leadership in ***business continuity***, disaster recovery, cyber resilience and related fields'

DRII has for some years now produced a summary document entitled '***Professional Practices for BC Practitioners***' (Professional Practices [**PP**]). The latest version is dated 2017 (please do check for any later version). This document is freely available from https://drii.org/ by following a simple registration process

Whilst the PP document is ***USA oriented*** it provides a useful list of what it terms 'continuity strategies' (NB: ***BC Strategy*** and ***BC Tactical Treatments / Solutions** etc.* are simply and ***JOINTLY*** known in the ***PP*** by the single term '***CONTINUITY STRATEGIES***'). To access and use the 'Continuity Strategies' section of the PP it us suggested that you:

- Register with DRII and then download the PP document
- Open the latter and go to section PP Four (4) - ***Business Continuity Strategies*** (page 15)
- Read the entire PP Four section (only 3 pages)
- Taking more time, now read again the paras headed by titles 'Objectives' and 'Professional's Role'
- Similarly re-read the paras headed by title 'Activities'
- Note that paras 1 through to 1.5 cover activities falling under what the PP terms as 'Operations'
- Note that paras 2 through to 2.4 cover activities falling under what the PP terms as 'Technology'
- Para 3 deals with supply chain type matters
- Para 4 covers 'consolidation of continuity strategies' e.g. to reduce costs and / or complexity
- Para 5 refers to the 'costs / benefits' analysis of proposed continuity strategies
- Para 6 deals with recommendation of continuity strategies and approval to implement

Note: BC operations as covered by DRII just above do ***not*** use the concept of MTPD. RTO is used instead to cover the ***combined*** meanings of MTPD and RTO (merged). It has been assumed herein that this concept applies across the USA. See DRII definition immediately below:

Recovery Time Objective (RTO) - (As used in USA?)

Time goal for restoring / recovering functions or resources based on the acceptable down time ***and acceptable level of performance*** in case of a disruption of op (The underlined words equate to MBCO)

IMPORTANT REMINDER: For the purposes of ***this*** guideline document (the one you are reading now [and in contrast to what has been written in the 'Note' at the bottom of the previous page]) MTPD and RTO ***are*** treated as separate concepts / calculations - and used as such accordingly

Some Examples of Typical 'BC Tactical Treatments / Solutions etc. - ***NOT*** from ISO sources (2)

BC Institute (BCI) - 'Good Practice Guidelines (GPG) 2018'

An extract from the above document's 'official' introduction reads as follows:

> '……………………The GPG is a comprehensive and independent BC knowledge source written by 'real world BC experts'. The GPG considers not just what to do, but why, how and when……………………'

It is available free to BCI members or can be purchased (for around USD $40) from BCI at:

https://www.thebci.org/training-qualifications/good-practice-guidelines.html

See 'Professional Practice 4 (PP4)' (somewhat confusingly entitled '**Design**') - for some excellent, generic examples of typical 'BC Strategy' and 'BC Tactical Treatments and Solutions etc.'

Note that instead of using the latter terms / titles, the GPG simply uses the term '***Solutions***' to mean the same thing

Note: As at 2022, a 'lite' version of the GPG 2018 was available, which could be freely downloaded provided an associated registration form was completed. Follow below link for more details:

https://www.thebci.org/resource/gpg-lite-2018-edition.html

Deliberately Blank

5 / 3B / **5** - Establishing Resource **Requirements**

Cross Reference ISO 22313 - 8.3.4

*Establishing Resource Requirements - **General***

- The organisation should determine (work out / estimate) the ***resources*** (sourced internally and externally) which it needs to provide / acquire in order to implement and operate the selected BC strategies and associated BC tactical treatments / solutions etc.
- + For the production of the associated ***BC Plans*** & ***Procedures*** etc.
- + For the setup, manning and operation of an appropriate ***Incident Response Structure***
- + For the setup and operation of an associated ***training*** and ***exercise*** regime
- + Anything else of significance re provision of resources for the BCMS

*The organisation should consequently **research** and **provide provisional costings** for*:

- The appropriate * ***manpower*** resources necessary to ** implement, operate, maintain, test and evaluate / review etc. the BCMS operation

  * ***Already covered*** in this guideline - see sub-section **4 / 2.5** - starts page 99

  ** ***Over and above*** those ***already*** assigned to the project so far

- ***Robust capabilities*** and associated ***processes*** etc. related to the significant logistical task of providing (sourcing, procuring, paying for, distributing / transporting, storing, maintaining etc.) the additional resources required (other than manpower) to fully support the BCMS operation

  As required, the above shall include acquisition of appropriate, external resources e.g. an alternate operating site(s); engagement of third party specialists and / or specialist organisations; use of an alternate workforce; arranging mutual assistance support agreements; establishing a 'work from home' (remote operation) capability etc.

- The appropriate '***administrative***' etc. (e.g. HR; Finance; Legal etc.) ***capabilities*** and ***processes*** etc. necessary to ***support*** **ALL** appropriate aspects of BCMS implementation and operation. All such processes etc. should be ***prioritised*** where so required - but should otherwise follow the appropriate normal business practices of the organisation (unless the 'urgency / criticality' of a particular BC response [anticipated or actually in action] ***dictates otherwise*** e.g. an influenza pandemic type scenario will probably fit the description of 'dictate otherwise')

- ***Objectives regarding 'response times'*** within which appropriate resources must be made available. This is particularly applicable to external resources

- ***Processes*** etc. (re provision of BC resources) with regards to 'other interested party / stakeholder assistance', 'strategic alliance agreements', 'mutual aid agreements' etc.

As mentioned earlier, the generic ***scope*** and ***choices*** of BC tactical treatments / solutions etc. (falling within an associated BC strategy scope) are typically related, in one way or another, to (single and / or combined) uses of:

- People (Having acquired / retained / maintained the necessary BC associated skills, experience, knowledge etc.)
- People (To man / operate 'Disruption Support Units' [latter is the BC related element of an overarching 'Incident Response Structure'])
- People (To Resume Activities)
- Information & Data (hard copy and electronic [soft copy])
- Buildings (premises / facilities), Workplaces & Associated Utilities
- Equipment (including Plant), Consumables etc. (Core supplies / goods / stock / machinery / tools etc.)
- Technology (predominately ICT and associated 'systems')
- Transportation and Logistics
- Finance
- Partners
- Suppliers / Supply Chain
- Other appropriate Stakeholders / Interested Parties (not already included above)
- Emergency Services (typically provided & funded by national / local government etc.)
- Any other appropriate resources (not already included above)

  Of course, all of the above are, in one way or another, ***resources***

Outcomes from the above should include:

- A consolidated list (with actual and / or estimated costings where appropriate) of all ***internal*** resources required to support the BCMS programme

- A consolidated list (with actual and / or estimated costings) of all ***external*** resources required to support the BCMS programme. Highlight (for review) any such resource(s) which might be difficult to obtain, be unavailable (for whatever reason) etc.

- A determination of ***how to best source external resources*** (e.g. consolidation, leverage [discounting] etc.)

- Providing TM with an ***evaluation report*** of the 'establishing resource requirements' task - together with any associated recommendations, potential problems etc.

- Obtaining agreement & approval from TM for ***consequential change(s)*** (if any) to any ***provisionally*** (pre-chosen) BC tactical treatments (and possibly BC strategy), as a consequence of any 'knock-on' effects which might subsequently become evident

- (Where necessary) - ***updating the projects list*** for the BC tactical treatments / solutions etc. implementation task

- ***Assisting in the determination*** of the structure and content of the Business Continuity Plan(s); establishment of the IRS etc. (which are to follow / are the next step [see sub-section 5 / 4 of this guideline])

Note 1: - the outcomes above should be ***provisional*** until such time as they are confirmed (or not) by TM - i.e. following the appropriate cost / benefit analyses (sub-section 5 / 3 / **6** of this guideline refers)

Note 2: - the 'resources' referred to above will typically by 'over and above' (additional to) those already approved and acquired (and / or pending acquirement) as already described and accounted for in earlier sections of this guideline document

*Establishing Resource Requirements - **Maintenance***

An appropriate ***maintenance*** policy should be established and operated to ensure that the outcomes of the '***establishing resource requirements***' task remain accurate, current, complete, are adequately documented etc.

*Establishing Resource Requirements - **Review***

A ***review*** of BCMS related '***resources required***' should be conducted whenever there has been ***significant change*** to a BC strategy and / or BC tactical treatment(s) / solutions etc.

Similar applies where there have been changes potentially affecting the provision of ***internal*** BCMS resources and also e.g. when a BCMS related ***external*** contract comes up for renewal; when an organisation's ***external environment*** changes significantly etc.

The above may result in subsequent changes / updates to the appropriate (associated) BC strategy and / or the BC tactical treatment(s) / solution(s) etc.

5 / 3B / **6** - **Costs / Benefits** Analysis

A 'costs / benefits' analysis should be conducted to assess the ***financial viability*** of implementing the provisionally chosen BC strategies / associated tactical treatments / solutions etc:

- Estimate the costs of implementing and maintaining chosen BC strategies / tactical treatments / solutions etc. (Note: This has probably already been accomplished via the steps already outlined further above. If not, the estimated costings should be made now)

- Validate that these estimated costs are commensurate with the 'amount' of the business / operation at risk (e.g. a million dollar BC strategy / tactical treatment would typically not be financially commensurate with protecting $100,000 worth of business etc. - ***BUT*** - may be so commensurate where the same business (operation etc.) has significant regulatory and / or safety and / or reputation and / or potential profit etc. type implications)

- Where cost is not considered commensurate with benefit - a review of the associated BC tactical treatment(s) etc. and / or associated BC strategy (strategies) will be necessary

Outcomes from all of the above (Sections 5 / 3B / 1 to 5 / 3B / 6) should deliver:

- A final 'chosen' ***BC strategies*** list
- A final 'chosen' ***BC tactical treatments*** / solutions etc. list
- A final ***project plan*** for implementing chosen BC tactical treatments / solutions etc.
- A final ***consolidated list of*** *(associated)* ***resource requirements***
- A provisional project plan (moving forward) for implementing ***BC Plans***
- A provisional project plan (moving forward) for setting up of the ***IRS***
- The ***most accurate estimates available of the costs*** involved in all of the above
- ***Provisional TM agreement with / approval of all of the above***

Costs / Benefits Analysis - ***Review***

A review of the ***costs / benefits analysis*** should be conducted whenever there has been a ***significant change*** in a BC strategy and / or BC tactical treatment(s) / solution(s) etc.

A similar review should be conducted where there have been e.g. changes which potentially affect the provision of ***internal*** BC resources; when an appropriate ***external*** contract comes up for renewal; when the organisation's ***external environment changes*** significantly etc. This review may result in changes to the appropriate BC strategy and / or the associated BC tactical treatment(s) / solution(s) etc.

Costs / Benefits Analysis - ***Maintenance***

An appropriate ***maintenance*** policy should be established to ensure that the outcomes of the 'costs / benefits' analysis remain accurate, current, complete and are adequately documented

5 / 3B / **7 - Final Agreement & Approval**

The desired outcomes here are:

- TM agrees to and approves the recommended BC strategies and associated BC tactical treatments / solutions etc.
- TM agrees to and approves the implementation, co-opting and procurement tasks related to the recommended BCMS resources requirements (including final agreement to and approval of the estimated costs / budget)
- TM agrees to and approves the implementation (project) plan associated with all of the above

- ***Moving forward*** from this BC Strategy phase, TM agrees to and approves the remainder of the provisional BCMS ***implementation*** (project) plan

*BC Tactical Treatments / Solutions etc. - **Review***

A ***review*** of 'in-force / active' BC tactical treatments / solutions etc. should be carried out at least annually - and / or following any significant change(s) to the associated parent BC strategy / strategies. ***Significant*** changes (from a BC viewpoint) in any of the following may also trigger such review (the list is not exhaustive):

- The ***skills*** required to undertake activities, processes etc.
- The ***premises*** at which the activities. processes etc. are undertaken
- The ***resources*** used by the activities, processes etc. (particularly ***ICT*** resources)
- The ***suppliers*** on which the activities, processes etc. are dependent
- ***Stakeholders*** and ***other interested parties*** who relate is some significant way to the activities, processes etc. (e.g. legal and regulatory)

An appropriate ***maintenance*** policy should also be established to ensure that active BC tactical treatments remain accurate, current, complete and adequately documented

5 / 3B / **8** - BC **Communications** with Stakeholders / other Interested Parties

As part of formulating a BC Strategy it is advisable to pre-plan (at least at a strategic level) for how 'communications' with stakeholders / other interested parties will be managed (and also ***who*** will manage and undertake them) in situations where an organisation's key products / services / operations suffer significant disruption

Such communications should be both internal (employees) and external (all other parties having an interest - who are possibly liable to a potential, adverse impact e.g. shareholders, customers etc.). Consider all types / formats of communication e.g. written (both hard and soft copy); spoken (verbal press releases; press conference); social media and similar etc.

In particular, careful planning should take place for communications ***with the media***. This can perhaps be best done via an overall ***'Crisis Communications Strategy'*** - however, this latter subject is beyond the scope of this guideline

Note - Where an organisation already has some form of ***emergency*** (crisis / incident / contingency) response plan in place - as do most airlines, airports etc. (see definition of 'emergency' etc. in the Glossary - found in separate [but related] guideline document CRPM Part 3 / Volume 1), it is more than likely that the 'requirement to communicate during crisis' will have ***already*** been planned for (typically as part of an overarching ***crisis communications strategy*** as mentioned above) and, if so, might be (relatively) easily adaptable for BC purposes

5 / 3B / **9** - Management of **Work Backlogs**

If an organisation fails to adequately plan to catch up on work backlogs caused by significant disruption - then the consequences of not so doing can be as catastrophic to the organisation as not dealing with the original disruption itself

One ‘formula’ reasonably assumed here is that it will take some 4 to 5 times the ‘normal’ processing time to recover a particular backlog i.e. one day’s loss would take four to five days to recover - assuming normal work hours plus 20 - 25% overtime

The methods typically used to ‘catch-up’ include:

- Use of overtime
- Sub-contracting to third parties / outsourcing
- Deciding ***not*** to catch-up should the consequences be deemed ‘acceptable’ (indicated typically e.g. via a cost / benefit analysis; consideration of risk appetite etc.)

Under the BCMS the likelihood and circumstances of work backlogs should be identified and documented and an appropriate and approved ‘* backlog clearance’ strategy (together with formulation of an associated, appropriate tactical treatment plan) devised, approved, resourced, documented, implemented, trained, exercised, reviewed and maintained

* Do not confuse ***this*** strategy (and its associated tactics) with ‘BC Strategy and associated Tactical Treatments / Solutions etc.’ - they are different!

5 / 3B / **10** - Address Activities, Processes ***not*** deemed **Critical** / **Critically Time-sensitive**

It will be recalled that an output from the ‘understanding the organisation’ task was to list those activities and procedures (together with their associated dependencies, resources etc.) which did not quite make it on to the list for consideration under BC Strategy etc.

It is now appropriate to ***review this list again*** to see if this ‘status’ (of all such activities etc. referred to just above) is still appropriate

If the status of an activity etc. remains unchanged, it should be reviewed again annually or when significant changes to the organisation might trigger such a review. A convenient time for annual reviews would be at the same time as the BIA review

Should a review identify that an activity, procedure etc. ***does*** subsequently require inclusion under BC Strategy - then appropriate action should be taken accordingly e.g.

- Assign MTPD, RTO and MBCO
- Include as part of the most appropriate BC strategy
- Assign appropriate BC tactical treatments / solutions etc.
- Ensure associated resources are provided
- Include in the BC Plan etc.

Should significant resources / costs be involved, then firstly seek approval to proceed from TM

A ‘**real life**’ example of an ‘**aviation related**’ **BC Strategy**

Note from author / owner of this guideline document

To date the author / owner of this guideline document has been unable to find a ***real life*** example re ‘aviation’ related BC Strategy (particularly for airlines and airports)

If users / readers are able to provide such an example(s) for inclusion here in this guideline document - please forward as per the email contact information shown in note 10, page 41 of separate (but related) document - CRPM Part 3 / Volume 1

All contributions will be gratefully received and the sources acknowledged herein

Rest of this page is Deliberately Blank

IMPORTANT REMINDER

Before continuing with Section 5 / **4** on the next page, it is strongly suggested that the serious / interested reader reviews the following definitions and associated information - found on the designated pages (listed a little further below together with definition titles) of the 'glossary' of ***separate*** (but related) document 'CRPM Part 3 / Volume **1**'

This is required as both 'CRPM Part 3 / Volume **1**' and the document which you are reading right now ('CRPM Part 3 / Volume **2**') have been designed (where possible / feasible) for use in an ***aviation*** related context - particularly re airlines (aircraft operators), airports and ground handling operators

Some commonly used RM / BC terminology (outside of the aviation context) ***is inconsistent*** with such aviation use - an example being use of the word 'incident' e.g. as used in the BC terms 'Incident', 'Incident Response Structure' etc.

Emergency / Crisis etc. - (CRPM Part 3 / Volume 1 - pages 72 to 73)

Incident - (page 75)

Incident Response Structure (IRS) - (pages 76 to 77)

Section 5 / 4 - DO - DEVELOPING and IMPLEMENTING the BCMS

ISO 22313:2020 / OPERATION / **BC Plans and Procedures** - 8.4

Despite the 'simplistic' ISO 22313 title immediately above, this sub-section **5 / 4** deals with:

- Development and documentation of an **Incident Response Structure**
- The ***Emergency*** *(Crisis / Contingency / Incident etc.)* ***Response*** Plan
- The ***Business Continuity*** Plan (General / Template - Guideline level)
- The ***Business Continuity*** Plans ([Specific] - * Individual Business Unit level)
- The ***Business Recovery*** Plan

* Otherwise known herein (in this guideline document ***only***) as '***Disruption Support Units*** - DSU'

INCIDENT **RESPONSE STRUCTURE** (IRS)

ISO 22313 - 8.4.2

Note: The original ISO 22313 of 20***12*** used the term / title 'Incident Response Structure' for this particular subject area. In the 20***20*** version they had usefully changed the title to simply '8.4.2 - **Response Structure**' (see important reminder' on previous page as to why this is useful). Unfortunately, in the very next para (8.4.2.1) they were back to using the words 'Incident Response Structure' again!!!

The EMERGENCY Response Team (i.e. **NOT** the BC Team [i.e. not DSUs])

Disruption is inevitable in some form, at some time to any organisation **BUT**……………… the first response priority of an involved organisation might **NOT** be business continuity related at all

Instead it might relate to responding to the ***immediate*** consequences of what leads to the disruption itself, ***where such consequences relate to a major emergency / crisis type situation*** - e.g. if danger of death **and / or** serious injury **and / or** major loss of property / facilities **and / or** significant financial loss **and / or** serious reputational impact etc. are all possible (and even likely in some circumstances)

Aviation Context

A direct and almost inevitable **side effect** of e.g. a catastrophic (mass fatality) aircraft accident (particularly at the accident airline's ***major hub*** airport[s]) - is very significant disruption to the accident airline's entire network operations

Such disruption typically arises as a result of e.g. closure of the associated airport itself (e.g. for a week or more in extremis); the parent airline's commercial call / contact centre(s) not coping with the vastly increased call volumes; airline website(s) etc. 'crashing' due the huge increase in 'hits'; public discontent / anger with the airline; brand / image / reputation problems etc.

However, before such airline (and the 'accident airport' too, of course - assuming [if the accident is 'on-airport'] that it will probably be closed for some significant time and, as such, have its own BC related problems to cope with) ***can even start to think about invoking their BC plans*** (assuming there are any?) **they obviously needs to respond to the immediate and shorter term consequences of the accident** (emergency) **itself** - many of which will involve EMERGENCY response + major humanitarian, welfare and logistical considerations etc.

Note - in the paragraph immediately above we are referring to the ***airline's*** (and airport's) immediate and shorter term responses and ***not*** to the response of the OFF-AIRPORT ***emergency services*** (fire and rescue; police; ambulance / medical etc.)

When planning for such response many airlines employ an ***emergency response planning manager*** (or similar title), who writes and maintains the airline's ***emergency response plan*** *(ERP)* - and also trains and exercises designated ***airline*** personnel in their anticipated emergency response roles, responsibilities and accountabilities. In this guideline ***only*** (i.e. the document you are reading now) such personnel are typically entitled the (name of airline) '***Emergency Response Team*** (ERT)'

Similar arrangements (typically with different but associated titles) apply to other types of aviation organisation e.g. ***Airports*** and ***Ground Handling Operators*** / *Agents*

*The **ERP** / **ERT** is **one** component of what is known herein as an * 'incident response structure'*

* **Reminder:** The term 'incident response structure' is ***not*** commonly used (if at all) in aviation related ***emergency response planning*** terminology i.e. it is typically used in a ***BC context only***

Coverage of the roles and responsibilities of aviation related ***ERTs*** is generally ***outside the scope*** of this guideline - and is thus mentioned herein for contextual & information purposes only

The Business Continuity Team *(continuing in the aviation context referred to above)*

As the nature of the ***disruption*** associated with an aircraft accident (such as the one referred to a little further above [we shall be using this same example throughout section 5 / 4]) becomes apparent, the airline's (*SEPARATE*) '***Business Continuity Team***' (BCT) will typically also be activated. The **BCT** responds to the ***disruption*** related elements of the incident ***only*** - as guided by the documented ***BC Plan*** (BCP) and its inclusive / associated procedures - or in an otherwise appropriate manner if no such procedures are documented e.g. due to the unique (and, therefore, unplanned) nature of some disruptions

*The **BCP / BCT** is **another** component of an 'incident response structure'*

The Business Recovery Team *(continuing in the aviation context)*

As the effects of the disruption begin to lessen (with time) it will be necessary to start 'converting' BC related ops back to 'normal operations' status. This process is known herein as '***recovery***' - and the team assigned to manage and operate it might be known as the '***Business Recovery Team***' (BRT) - as guided by the documented ***Business Recovery Plan*** (BRP)

*The **BRP** / **BRT** is a **further** component of an 'incident response structure'*

Reminder - detailed coverage of the ***BRP*** / ***BRT*** is generally ***outside*** the scope of this guideline document - and is mentioned herein for contextual & information purposes only

Command, Control, Co-ordination & Communication (C4) ***Team***

As per what has been written so far, we now have 3 different teams + 3 different plans which, during emergency / crisis and ***associated*** disruption response operations, are all interdependent to a degree - and thus need to interrelate and interact in an effective, efficient, expeditious, cohesive and consistent manner (e.g. via use of standard operating procedures; joint training and exercising etc.) which will be of most benefit to the parent organisation

Accordingly, a fourth (overarching / strategic) team is required to direct / manage this interrelationship and interaction - and (in this guideline document ***only***), is known as the '***Command, Control, Co-ordination and Communication*** (C4) ***Team***'

*The **C4 team** is the **last** component of a typical 'incident response structure'*

If an *incident response structure* as described above (or similar) has ***not*** been established, the best that could generally be managed by most aviation related organisations (responding to a significant crisis causing associated major disruption) might be termed '***ad hoc***', '***on the hoof***', '***winging it***', '***handle it as we go***' etc. - all of which are highly undesirable e.g. the latter might lead to even more disastrous consequences for the organisation, than those caused by the emergency / crisis and associated disruption in the first place

Notes

- The IRS structure is shown in diagrammatic form in figure 22 - page 227
- The IRS component teams as described above will obviously not act in isolation from each other. It is expected that there will be some overlap of roles & responsibilities in some areas - and there will always be the need for communication, co-ordination, co-operation, consistency and mutual support
- Some of the above teams might operate from different geographic locations - so methods of reliable & speedy communications (& possibly transportation) might be considerations
- For smaller organisations some (or total) merging of the 4 teams above will be required e.g. the same team can conduct both emergency and BC operations and share C4 resources

- For the smallest organisations, the entire roles and responsibilities of the 4 teams above might need to be assigned to just e.g. two or three persons! This is obviously far from ideal - but there may be little or no choice in the matter. The ‘one / single person’ team should be avoided if at all possible - for obvious reasons (e.g. single point of failure)

- In many organisations (particularly with low manpower resources) *the Business Recovery Team* will, in fact, not be a separate ‘team’ at all. Rather, the personnel charged with *business recovery* operations will be one and the same as those conducting *BC operations*

- One suggested method of applying C4 can be accomplished by ***each*** team (ERT, BCT, BRT) having its own specific (self-contained / embedded) ***tactical*** **C4** function. Appropriate (*pre-prepared*, *trained* and *exercised*) plans and procedures should then be used by these tactical C4 teams to ensure that the associated inter-dependencies, inter-relationships, interactions and inter-communications function consistently, in the best interests of the organisation as a whole

  In the above ‘method’, an independent and overarching ‘top management’ ***strategic*** C4 team should additionally be ‘on immediate call’ to resolve any situations which are beyond the capabilities of the ***tactical*** C4 teams to resolve e.g. a conflict of interests over use of a shared resource. Otherwise this method of C4 should not significantly involve top management - allowing the latter to concentrate e.g. on managing stakeholder / other interested party relationships; manage strategic matters related to the accident / disruption; deal with crisis communications, regulators, shareholders etc.

IMPORTANT NOTE

In most organisations, ***internal*** manpower resources dedicated to emergency / crisis response ***and*** BC response will (in theory at least) be provided (in the main) by trained but unpaid ***volunteers***

(A small number of organisations have tried in the past to include such responsibilities within ‘official’ job descriptions across their workforce - ***typically with undesirable consequences*** as no extra payment / remuneration was generally forthcoming - so this option is probably best avoided)

Such volunteers should be treated with consideration and respect - and TM should regularly recognise their contribution in one way or another e.g. as part of any ‘recognition and rewards’ scheme

For BC exercise planners, make ‘no notice’ exercises the rare exception. For BC trainers, make the subject as interesting and relevant as possible - and deliver the training in as short a time frame as is commensurate with achieving the training objectives

In the aviation context - some airlines have already used attractive incentives to ‘maintain the interest’ of their volunteers - e.g. competitions with prizes such as all expenses paid holidays to luxury destinations; e.g. the offer of first or business class travel to any destination on the airline network (subject to load) each time refresher training was undertaken; e.g. the holding of free (i.e. food, beverage, entertainment, raffle prizes etc.) annual ‘social functions’ for all volunteers etc.

Now also see again the ‘**IMPORTANT NOTE**’ starting on page 102. The latter is targeted in particular at the ***Incident Response Structure*** (and potential /associated [lack of] manpower resources in particular). Appropriate solutions **MUST** be found - if so required

A Typical **I**ncident **R**esponse **S**tructure (Aviation Related Scenario)

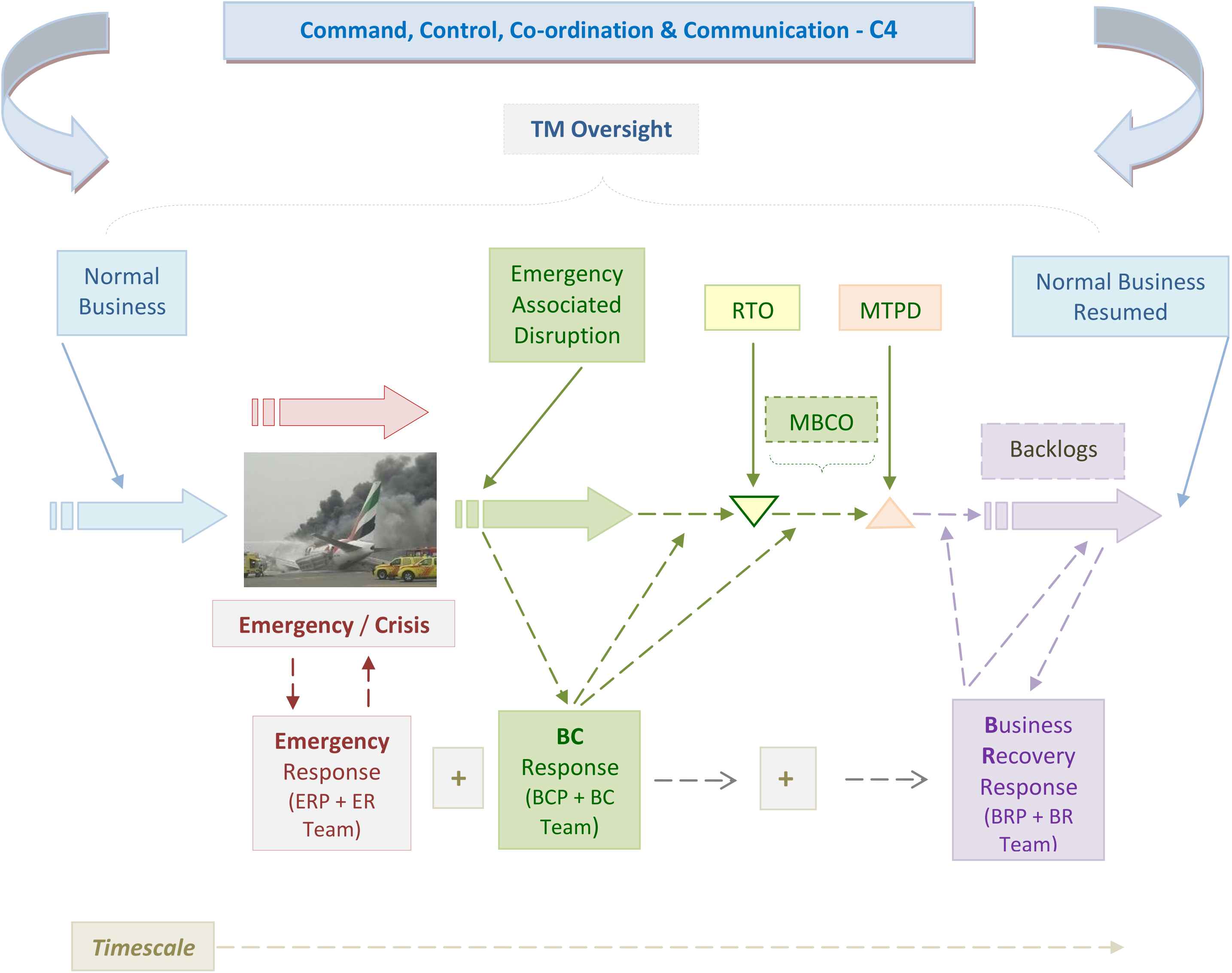

Command, Control, Co-ordination & Communication - C4
TM Oversight
Normal Business
Emergency Associated Disruption
RTO
MTPD
Normal Business Resumed
MBCO
Backlogs
Emergency / Crisis
Emergency Response (ERP + ER Team)
+
BC Response (BCP + BC Team)
+
Business Recovery Response (BRP + BR Team)
Timescale

Fig **22** - **Typical IRS** - Depending on nature of incident, timescale can run from minutes to hours; from hours to days; from days to weeks and, in extremis, from weeks to months or even longer. Time and functional overlaps of **ER**, **BC** and **BR** operational functions are to to be expected

- ***Emergency / Crisis*** Response - immediate / short to mid-term e.g. execute **ERP**; evacuation; humanitarian; welfare; damage assessment & containment; crisis communications; invoke **BCP** etc.
- ***Business Continuity*** Response - short / mid to longer-term e.g. execute **BCP**; maintain / resume key operations at pre-designated levels; stakeholder / interested party communications; invoke **BRP** etc.
- ***Business Recovery** Response* - mid to longer term e.g. execute **BRP**; damage repair and / or replacement; deal with work backlogs; maintain / resume normal service levels etc.

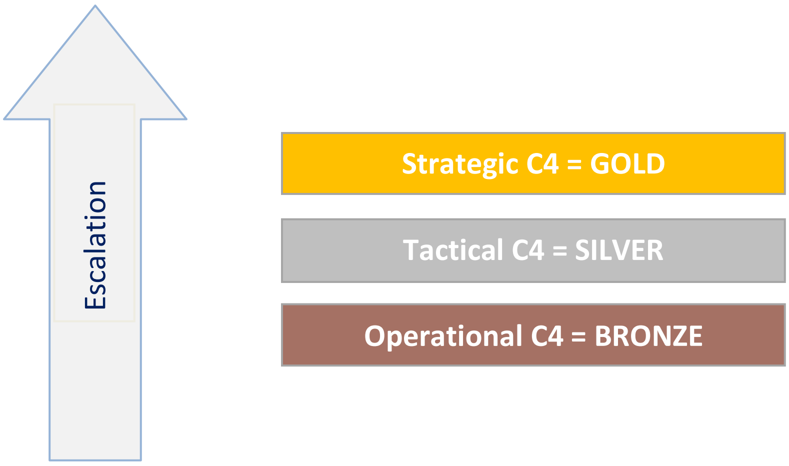
IRS - Levels of Command, Control, Co-ordination & Communication (C4)

C4 systems typically operate at three levels of responsibility and accountability - i.e. strategic (top level), tactical (intermediate level) and sub-tactical / operational (lower levels)

For ***airline*** emergency / crisis response ops, strategic C4 is typically exercised by TM; strategic to tactical C4 by a higher to middle level management group and operational C4 by lower management and non-management staff (all should be competent and experienced + have ready access to 'everything that they might need' in order to 'do what they must do' etc.)

Similar typically applies to equivalent ***airport*** and ***ground handling agent*** operations and is equally applicable to **BC** and **BR** operations

This C4 concept is so logical that it is generally followed (to some degree & in one form or another), by all types of organisations (including the military), world-wide e.g. in the USA this countrywide C4 concept, as typically related to emergency / crisis response, is known as the 'Incident Command System - ICS' which, in turn, is a sub-component of the 'National Incident Management System - NIMS'. In UK, Ireland, UAE, Oman and a small number of other countries, the C4 system is colour coded and entitled as shown below:



For more info on the ***ICS***, ***NIMS*** & ***Gold*** / ***Silver*** / ***Bronze*** C4 systems (referred to above) click ***HERE***

When the destination webpage opens, scroll down until you find the info article entitled:

- Info Article - Typical **Crisis Response Command & Control Systems** (national level)

Click on it to open and read

IRS - Alerting & Activation

The various teams / personnel comprising the IRS are obviously not on 24 / 7 / 365 call - e.g. simply waiting for the time when their services will be required for crisis & continuity response i.e. they are actually doing their 'normal' jobs or on days off, vacation, business travel, sick etc.

However, to be of any use at all, some key element (mainly ***initial*** assessors / decision makers) of the IRS needs to be capable of being very rapidly alerted and activated. Consequently, some form of 'guarantee' is necessary such that at least a pre-defined ***minimum required contactability & manning component*** of the IRS will be available for 'almost immediate' duties - assuming that the nature of the organisation's key operations so requires (which applies in reality to many [if not most]) ***airlines*** & ***airports*** etc. - particularly those which ***operate 24H***)

This latter typically entails a ***limited*** degree of '24H on-call' capability for ***designated*** key team members - and can be accomplished in a number of ways (which are beyond the scope of this guideline, and are mentioned for contextual and information purposes)

Many airlines, airports, GHAs etc. use their normal business 'operations control (ops management) centres' (or equivalents) to initiate the primary alerting & activation system associated with an emergency / crisis or similar disruption event and, where so required, the (trained and exercised) 'senior manager(s) on duty / on-call' will typically conduct the ***initial*** elements of assessing and managing the emergency / crisis and / or continuity response, until relieved by the **ERT** and / or the **BCT**

Whilst there is typically a degree of urgency / immediacy in alerting and activating the **ERT**, the **BCT** is typically alerted / activated at some later stage (perhaps some hours or so but possibly even days [or even longer] later) - depending on the estimate of when any associated disruption will begin to adversely impact on key (prioritised) operations, services, product etc.

Conversely, **business recovery** operations might not start for days, weeks or even months e.g. replacement of a destroyed building facility for the latter timescale

Alerting & activation can be achieved in several ways - the most basic of which is 'person to person / group of persons' - using some form of alerting cascade tree (see typical example of how this works on next page)

At the other extreme are sophisticated ICT (automated) alerting systems capable of alerting thousands of pre-selected teams / persons in just minutes. Such systems are, in the main, supplied by commercial entities, and typically leased to 'customers'. Relatively speaking such a system is not too expensive (to lease and operate) and, in this 'modern' world might be considered as a high priority necessity. For an example, follow this link

Note - other than what has been written above, alerting and activation methodology in detail is ***beyond the scope*** of ***this*** guideline document. It is suggested that the user / reader studies ISO 22313:2020 / clause 8.4.3 - 'Warning & Communication' - if more information on this subject is required

'Cascade Callout Tree' Alerting System - Typical Example

One of the simplest types of (manual) alerting system would require the person commencing the alerting process (e.g. person **A**) to make ***telephone*** calls to persons **B**, **C**, **D**, **E** and **F** etc. In turn, person **B** would then pass on the alerting message to persons **1**, **2**, **3**, **4**, **5** etc. (See Fig. 23 diagram further below)

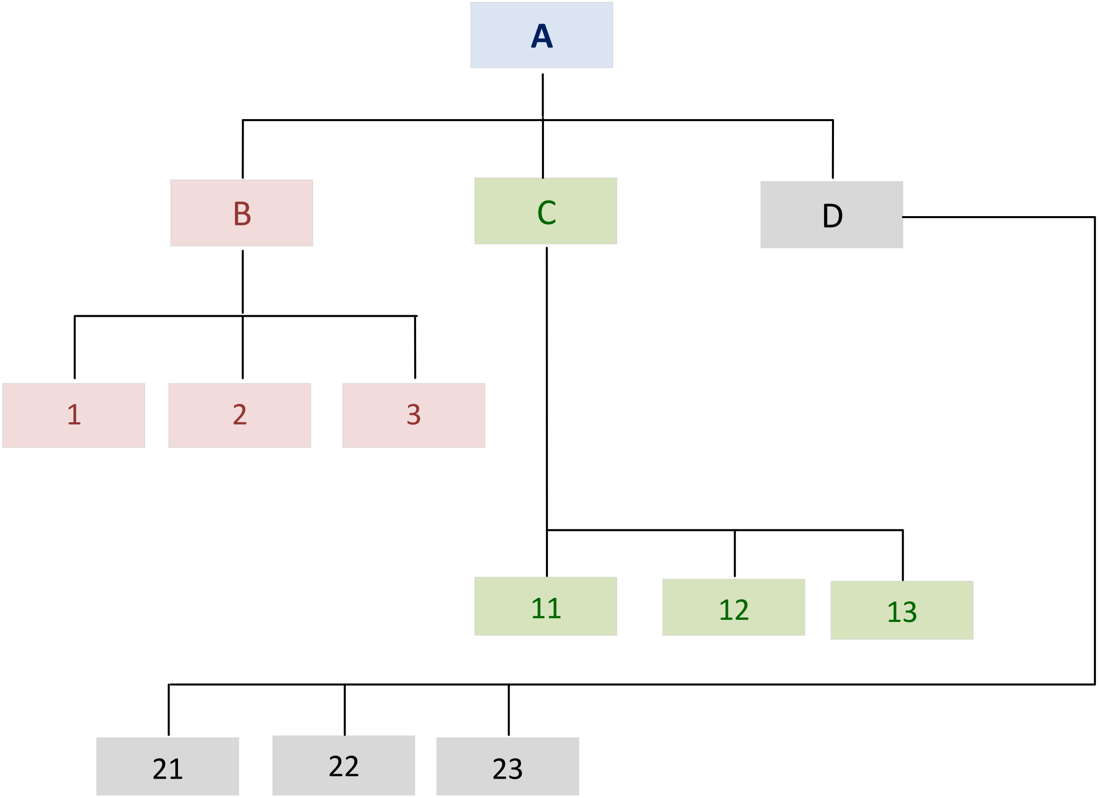
Person **C** would pass on the alerting message to a different group of persons than those contacted by person B - say persons 11, 12, 13, 14, etc. and so on - until the full list of persons to be alerted has been contacted

At the 'letters' level shown above and below (B, C, D, E etc.) - if a person to be contacted does not respond, then the person 'doing the contacting' (person A in this case) takes over the alerting job for that (non-responding) person, making a note of who could not be contacted

At the 'numbers' level shown above and below (1, 2, 3, 4, 5 etc.) - if a person to be contacted does not respond, then the person 'doing the contacting' simply moves on to the next contact in that particular alerting group, making a note of those unable to be contacted

The system's main advantage is its simplicity. Its main disadvantage is that it can take considerable where a large numbers of persons need to be contacted - and requires personal contact details (office, home and mobile telephone numbers etc.) and the associated procedures to be constantly maintained

Fig **23**



IRS - Modus Operandi (i.e. how a typical IRS might work in practice)

A good IRS will typically operate in a manner which will include the following generic elements - ***each of which can be applied to any*** / ***all of the individual IRS teams*** - as required (the below list is not exhaustive i.e. it is representative only):

- Classify the incident situation's scale / severity e.g. **RED** (high severity); **ORANGE** (medium severity); **GREEN** (low severity) etc.
- Initiate the pre-prepared alerting and activation system
- Invoke pre-prepared plans, checklists etc. - to the extent required by the situation
- Establish a reliable and accurate inbound Information flow re the 'situation'
- Collate and prioritise incoming information and convert it to a constantly updated situational 'Big Picture' account of 'what is going on' etc.
- Ensure that those needing to acquire and retain the Big Picture (decision makers) do so
- For the latter assess (and continually re-assess) the Big Picture situation
- Make appropriate decisions and issue associated instructions to those designated to execute them
- Monitor progress of execution of the decisions referred to immediately above
- Escalate issues (e.g. to TM) where deemed necessary
- Communicate - both internally (within the organisation) and externally (particularly with the 'public', 'authorities', the 'media' etc.)
- Where 'victims' are involved e.g. death, injury (physical and / or mental) & similar impact human consequences - humanitarian assistance and welfare considerations - together with effective, efficient and consistent communications - ***are paramount***
- Keep communicating (whilst ensuring that all communications are consistent)
- Look after welfare of IRS team members & other associated personnel
- Maintain a written record of all significant events (keep such records)
- Decide when to stand down the IRS
- Compile 'lessons learned' and ensure that associated 'action points' are dealt with

Note - The military, emergency services etc. operate a C4 structure (see page 228) - where one is typically directed in what to do - or one directs others in what needs to be done. Organisations more familiar with managing 'anything' via ***debate*** / ***consensus*** ***WILL*** be at serious disadvantage if trying to apply this latter management style to an IRS. Training and exercising in the 'military etc. style' method of IRS C4 management will go some way to overcoming this potential limitation. (NB: military style C4 does ***not*** mean that there is a lack of initiative or flexibility - far from it. 'In the right hands' - effective and efficient military style C4 relates directly to the concurrent management / combination of both)

IRS - Resources

IRS related resources should be planned for, documented, approved, budgeted, procured and 'stored' when completing (or as a consequence of completing) the 'Business Continuity Strategy'. One important resource ***ideally*** required by any IRS is the availability of suitably sized, located and equipped C4 primary and backup (alternate) operating facilities / locations

Note - establishment and management of C4 facilities is ***beyond the scope*** of this guideline document

IRS - BC **PLANS** & associated **PROCEDURES** etc. (in more detail) ISO 22313:2020 - 8.4 refers

The organisation should put in place and document (in a 'business continuity' plan[s]) those procedures, processes, information etc. which provide for overall control and management of its response to a disruptive incident. This includes (amongst other matters) resumption of key / prioritised 'activities' (to pre-designated MBCO levels) - within pre-designated and associated RTOs. Such 'business continuity' procedures etc. should account for and establish the appropriate internal and external communications protocols required and also be:

- **Specific** - with regard to the immediate and subsequent steps to be taken
- **Flexible** - so that they may be used to respond to unanticipated threat scenarios, changing internal and external conditions etc.
- **Focused** - so that they may clearly relate to the impact of events that could potentially most disrupt specified operations. They should also be further developed as required
- **Effective** - in terms of minimising the consequences of disruption through implementation of appropriate (business continuity related) mitigation strategies

THE EMERGENCY RESPONSE PLAN (ERP)

An **ERP** (which is ***NOT*** the same thing as a BC Plan - BCP) is used (where appropriate and ***in the context of the document you are reading right now***) to respond to and 'manage' the immediate and shorter term (***emergency / crisis related specifically***) consequences of an associated disruption event (as relevant) - and thus ***NOT*** to any associated / consequent ***business continuity / business recovery*** type matters. It is thus implicit that an ERP is invoked in response to a major crisis / emergency, predominately where some element of 'danger to life' (or similar severity impact) is / was a factor

Reminder - the subject of the ***ERP*** is mentioned at this point for 'contextual' and information purposes ***only***

THE BUSINESS CONTINUITY PLAN (BCP)

Note - where the term, 'business continuity plan' is used in what follows, it can be assumed that all associated / required etc. 'procedures, processes etc' are also included

There are various ways of writing / producing **BCPs** - typically dictated by an organisation's business type, size, complexity, operating environment etc. As our 'role model organisation' for this guideline is a 'generic' medium to large sized entity with relatively complex issues involved, a proposed guide follows below - which should be suitable for how any such associated BCP might be produced:

A BC Plan comprises documented procedures, processes etc. which:

- Identify the immediate (associated) steps to be taken
- Assist with timely decision-making
- Is sufficiently flexible to deal with unanticipated threats, changeable situations etc.
- Focus on the anticipated impacts of disruptions
- Align with selected BC Strategies (+ associated tactical treatments / solutions etc.)
- Clearly identify associated roles, responsibilities etc. regarding associated matters

MASTER *BCP*

The **Master** BCP is an overarching, documented plan providing BCP generalities, required information, implementation guidelines, templates (*latter two used to guide preparation of* ***subordinate*** *'Individual Business Unit' level BCP plans*) and necessary 'authorisations.' The master BCP is essentially a 'strategic' document and apart from what has been mentioned already and what is mentioned further below, should contain little else

As the master BCP will be approved by TM - the 'authorities' contained in it are binding on any of the organisation's individual business units (**IBU**) required to participate in the BCP (appropriate [brief] details of such IBUs also needing to be documented in the ***master*** BCP)

> Note - At a 'drill down' level, designated IBUs are required to produce ***their own*** 'subordinate & individual' BCPs, related specifically to the particular '***BC tactical treatment*** / *solution etc.*' responsibilities assigned to them. Before this can be accomplished, appropriate training must be provided to designated IBU staff. The latter should also periodically exercise their own BCPs - both individually and in conjunction with larger scale 'organisational' exercises involving other IBUs, external participants etc. IBU BC Plans shall be continually maintained and reviewed on a regular, published cycle

Items such as BC ***Objectives***, ***Policy*** (including 'scope') and ***Strategies*** should also be included in the master BCP - along with the ***condensed*** rationale for what the document is basically meant to achieve i.e. the ***much abbreviated*** conclusions of the 'understanding the organisation' task + anything else thought to be appropriate

The Master BCP will typically be produced and maintained by the foremost BC 'expert' within the organisation e.g. the BC Manager or equivalent person. However, where circumstances so dictate - an external specialist in (aviation related) BC matters may be engaged accordingly

This strategic document should also contain brief details of any other ***higher*** level response plans associated with ***disruption*** in a significant way e.g. the internal and external communications plans designed to protect brand, image and reputation and to communicate with stakeholders / other interested parties

Individual Business Unit *(Disruption Support Unit) BCPs*

Note - the terms '***individual business unit***' and '***disruption support unit - DSU***' may be regarded as being synonymous / interchangeable when used in this guideline document. However, (and hereafter in this guideline document) the term '***disruption support unit***' is preferentially used. See pages 100 to 104 - The '**Workers**' etc. - for a detailed description of DSUs

It is essential that ***each*** DSU *has its own, individual* (subordinate to the master BCP) *BCP, specific to its own BC accountabilities, responsibilities* etc. - if for no other reason than if these BCPs were contained in just a single, overarching BCP document for the whole organisation - the document would probably be very large, unwieldy - and no one would ever read it!

Of course, there are more practical reasons for producing specific / individual DSU BCPs - the main one being:

‘…………..who better to produce the required ‘tactical’ BCPs than the ***specialist and expert DSUs***, most appropriately related / experienced etc. (because of ‘what they do’ during ***normal*** ops) to the particular BC tactical treatment / solution etc. *(as it applies to a particular, associated activity, process etc.)* under consideration……………’?

For example:

- The ***ICT*** *DSU* produces its own subordinate (tactical) BCP to deal with disruption / continuity issues relating to the vitally important contribution of ICT technology to almost all organisations today - and the considerable (disastrous in some circumstances) consequences should this not be adequately accomplished
- The *‘Facilities’ DSU* produces a tactical BCP dealing with e.g. matters relating to buildings, physical and technology related security of premises, utility supplies, cleaning & catering services etc.
- The *‘ecommerce’ DSU* (in conjunction with the ICT and Corporate Communications / PR DSUs) formulates BC tactical treatments / solutions etc. for how it will maintain the organisation’s website(s) and social media capabilities e.g. under extremely heavy load (hits) related to a major emergency / crisis impacting on the organisation
- In an ***airline*** context:
    - The airline’s ***Operations Control Centre’s*** (OCC) *DSU BCP* should e.g.
        - Include procedures for maintaining the continuity of flight operations in general
        - Include procedures for initially invoking (alerting & activating) the organisation’s BC response
        - Include procedures for tactically managing the entire BC response until such time as the **BCT** can take over this responsibility
    - The ‘***crewing section***’ *DSU* (if not part of OCC) should e.g. have tactical BC plans for continuing to provide operating crew
    - The ‘***aircraft engineering***’ *DSU* should deploy tactical measures to ensure that aircraft servicing & maintenance ops can resume / continue
    - ***Reservations offices, call centres, ticket shops / desks*** etc. should e.g. have tactical BC plans etc. in place to deal with vastly increased enquiries from the public *(as, following a catastrophic aircraft accident, an airline’s call centre(s) etc. will be swamped with calls for information; to cancel / rebook flights etc.)*

- ***For an airport context*** - many (airport) ***DSU****s* will require similar (to the airline) tactical BCPs covering their own, specific accountabilities / responsibilities related to e.g. closure of an airport for a protracted period due fog / snow / ice etc.; disruption of ICT; loss of utilities; loss of navigation aids; disruption / loss of air traffic services; loss of an airport terminal(s); industrial action; natural disaster; unlawful activity etc.

- …………………………………………and so on

Administration of DSU BCPs

- *DSU* BCPs should be as small and simple as possible - but always commensurate with the required intent of 'what is required'. (A small plan is of no use if it excludes essential / highly desirable information. Conversely, no one will read an oversized plan unless ***most*** of its content is ***very*** relevant [unlikely] to the reader)

- BCPs can be in both hard and soft copy format if desired. As an absolute minimum, hard copy is always required. At least two ***hard*** copies of ***each DSU's BCP*** must be stored in a reasonably & relatively quickly accessible, secure and geographically appropriate 'off-site' location

  Soft copy DSU BCPs must be additionally available via backup systems / applications / networks which can ***reliably*** be accessed ***separately*** *and* ***remotely*** from the primary method(s) of data storage within the organisation

  'Soft copy only' BCPs ***are NOT acceptable***

  The ideal location to store soft copy DSU BCPs might be e.g. an appropriately accessible and secure 'sharepoint' site or similar e.g. in the 'cloud' (ideally both). As an additional backup, the organisation's intranet (if any) might be used - provided appropriate personal data is first removed and that a separate, secure and robust backup data, power etc. source is available to support it

- ***Each DSU BCP should have an 'owner'*** *and separately -* ***an 'approver'***. The owner (subject matter expert) actually produces (writes) and maintains the plan under the guidance of the organisation's BC manager (or equivalent person) …………and the approver (senior line manager of the specific DSU) ensures that the plan is 'suitable (fit) for purpose' in all respects with regards to said specific DSU requirements

- ***DSU BCPs shall be controlled documents*** (version control, contents list, list of effective pages, revision procedure etc.)

- ***DSU BCPs containing 'sensitive' data*** must be suitably protected / safeguarded

- ***DSU BCPs are subordinate*** *(but independent)* ***components*** of the ***master*** BCP

Where feasible, ***each DSU*** should identify (in its own ***tactical*** BCP document) an alternate operating location (suited to that particular DSU's particular requirements - including 'work from home / remote operations' considerations where appropriate) - should access to normal work location(s) be denied

Typical (**DSU**) ***BCP Contents*** *(this list is* **not** *to be considered exhaustive)*

- ✓ Details of the BCP's '***owner***' and (separately) its '***approver***'. Each should sign and date the document accordingly to the effect that it is 'fit for purpose' and 'approved for use' respectively
- ✓ The usual '***controlled document***' requirements e.g. glossary, revision procedure, contents page etc.
- ✓ ***Purpose & Scope***
- ✓ ***Objectives*** + associated measures of success (or otherwise) in achieving same (particularly re the appropriate BC tactical treatments / solutions etc. to be applied)
- ✓ ***General Background Information*** / introduction
- ✓ ***Alerting & Activation System*** details (Invoking the Plan - including details of which persons are authorised to action the 'invoking')
- ✓ ***Identities*** (with roles, responsibilities, accountabilities, nominated alternates / deputies, contact information, terms of reference etc.) ***of those required to deliver and operate the plan*** i.e. those persons who, together, comprise the particular DSU
- ✓ ***A prioritised list of activities, processes etc. and supporting issues*** (e.g. resources) ***for which a particular DSU has been assigned business continuity responsibilities*** (tactical treatments / solutions etc. and similar) under the overall BC Strategy. Where appropriate, each item listed should include its associated MTPD, RTO & MBCO

Reminder *- for simplicity, only* ***MTPD*** *&* ***RTO*** *have been considered in this guideline document. However, when / if planning BC strategy for recovery of* ***information and data*** *type assets,* ***MTDL*** *&* ***RPO*** will additionally apply *- and* **must** *be accounted for accordingly*

- ✓ ***For each activity, process etc. and supporting issue listed immediately above - BC procedures are to be prepared, documented and approved***. Each shall describe, in the appropriate detail, how the specific DSU will maintain the assigned level(s) of continuity i.e. how it will resource, apply, manage, monitor, measure & review its assigned BC tactical treatments / solutions etc. (See again 'Objectives' further above)
- ✓ For each BC tactical treatment / solution etc. procedure listed immediately above - ***a corresponding checklist shall be produced & documented***
- ✓ A ***prioritised*** list of ***internal*** and ***external interdependencies*** and ***interactions***

- ✓ ***How external parties*** (which directly support the particular DSU BCP) ***are to be incorporated*** (if they so agree) ***into the specific DSU's continuity preparations and response plans***. This particularly applies to external suppliers. Consider associated use of contracts, service level agreements etc.

- ✓ ***An 'escalations' process*** for situations where the DSU requires higher level input, direction, support, resources, conflict resolution etc. (e.g. crisis communications [internal and external])

- ✓ ***How information flows*** (in and out of the DSU) ***are to be managed***
- ✓ ***Communications requirements and procedures***

- ✓ ***A comprehensive, current, indexed and otherwise well maintained telephone*** (and other types of contact) ***director***y, prepared specifically for use in such operations e.g. it should contain details of ***all*** key organisational staff relevant to the particular DSU, other key stakeholders including external suppliers and customers, the emergency services, regulators, other interested parties / stakeholders etc.

- ✓ ***A list of vital documents, information and other resources required to conduct the BC operations allocated to the DSU***

- ✓ ***Details of an alternative location(s)*** - both for operation of the DSU where the use of the primary facility is denied - and also for separate and safe storage of vital, supporting resources - as appropriate. (Include e.g. 'rendezvous' locations where staff can gather prior to proceeding to alternate locations - together with details of tentative transportation information [if appropriate])

- ✓ ***How 'people'*** (staff / employees, families & others) ***type issues are managed and supported during continuity operations*** e.g. welfare / humanitarian, health and safety, shift planning, catering etc.

- ✓ ***Pre-planned 'salvage' arrangements made for recovery of damaged documents, facilities & resources*** (where possible) - caused by disruption e.g. flood, fire etc.

- ✓ ***Specific guidelines on BCP training, exercising, maintenance, monitoring, improving and reviewing*** - as they apply to the particular DSU itself

- ✓ ***Procedures for stand-down and other post BC response operations*** e.g. hot and cold wash-up meetings (debriefs) with e.g. corrective action lists and responsibilities (what can we do better next time?), recognition and rewards (e.g. an official 'thank you'; time off granted; financial and similar rewards) etc.

- ✓ ***A easily managed list of essential cross-references***

DSU *BC Plans* - ***Production / Implementation***

After appointment of a DSU’s BCP owner and (separate) approver - the DSU BCP shall be produced, maintained etc. (i.e. by its ‘owner’)

The BCP ***master*** document is typically used for higher level guidance in this task. Furthermore, the person who ‘manages’ said master document (i.e. the organisation’s BC manager or equivalent person) should provide associated ‘one on one’ personal support and guidance (including formal training if necessary) to said individual DSU BCP ‘owners’

When the first draft of the DSU BCP is complete it should be fully reviewed (together with feedback) by firstly the ‘approver’ and subsequently the organisation’s BC manager or equivalent person

Following successful incorporation of (feedback provided / required [if any] as per above) actions by the DSU BCP owner - the updated DSU Plan is then distributed within the associated DSU (and also amongst all other appropriate stakeholders / interested parties) for comment

Where necessary, the plan is then further updated, ‘approved’ and distributed again (in its ‘final’ version for now) to those that need to use it (or be aware of it) for BC purposes

The DSU can then progress to the ever on-going tasks of DSU BCP training (initial and recurrent), exercising, maintenance, monitoring, reviewing and improving

DSU *BC Plans* - ***Training***

Initial training of all DSU staff will initially be carried out by the BC Manager or equivalent person - with the appropriate DSU BCP owner and nominated alternate (deputy) persons ‘understudying’ (train the trainer)

Subsequent training should be performed ***internally*** by the DSU BCP owner and / or nominated alternate person(s)

Note: - Pedantically, it is only necessary to produce DSU BC plans, procedures and checklists etc. - which cover response to ***pre-specified*** disruptions, as documented in / under the parent organisation’s BC Strategy (ies)

However, a BC plan meant to deal specifically with one particular area of disruption e.g. IT (ICT); natural disaster; facility fire etc. - is often capable of being ‘adapted’ to other (***unplanned*** for) disruptions, of a broadly ***similar*** nature - and this latter should be implemented accordingly, where such circumstances exist and so permit

Note: - it is recommended that the user / reader also studies ***all*** of ISO 22313:2020 - clause **8.4**

Cross Reference - ISO 22313:2012 / **Procedures** - 8.4.4.3

ISO 22313:20***12*** (i.e. the previous version) referred to '*specific types of procedures*' (clause 8.4.4.3 of that 2012 version refers) - presumably with the intent (although this is not explicitly stated) that same should be included in BCPs???

These '*specific types of procedures*' (by ISO 22313:20***12*** clause number [equivalent 20***20*** version clause numbers shown in brackets] & title) were:

- 8.4.4.3.1 - Incident / Strategic Management Procedures (8.4.4.4 in the 2020 version)
- 8.4.4.3.2 - Communications Procedures (8.4.4.5 in the 2020 version)
- 8.4.4.3.3 - Safety & Welfare Procedures (8.4.4.6 in the 2020 version)
- 8.4.4.3.4 - Salvage & Security Procedures (8.4.4.7 in the 2020 version)
- 8.4.4.3.5 - Resumption of Prioritised Activities Procedures (8.4.4.8 in the 2020 version)
- 8.4.4.3.6 - The procedures for resuming activities should identify the ICT systems upon which such resumption relies, together with referencing the associated ICT continuity procedures required so to do (8.4.4.9 in the 2020 version)

The requirements of clause 8.4.4.3.5 (2012 version) / 8.4.4.8 (2020 version) have already been covered in this guideline document (i.e. the document which you are reading now). Same applies to clauses 8.4.4.3.6 / 8.4.4.9

All other clauses (both versions) above are ***outside the scope*** of same - as per the declaration just a little further below. However, (separate) study of such clauses (2020 versions) is nevertheless recommended, where the user / reader considers that such a course of action might be appropriate to his / her own organisation's specific circumstances

Declaration:

Scope of *ISO 22313:2020 - clauses 8.4.4.4 to 8.4.4.9* - with regards to ***this*** Guideline Document only

The subject of ***emergency / crisis*** (incident / strategic) ***management*** - other than directly relevant BC management related matters - is ***beyond the scope*** of this guideline document

The subject of ***communications procedures*** is ***beyond the scope*** of this guideline document

The subject of ***safety & welfare procedures*** is ***beyond the scope*** of this guideline document

The subject of ***security procedures*** is ***beyond the scope*** of this guideline document

The subject of ***salvage etc. procedures*** is ***beyond the scope*** of this guideline document

THE BUSINESS RECOVERY PLAN (**BRP**) Cross Reference - ISO 22313:2020 / **Recovery** - 8.4.5

Note - The subject of Business ***Recovery*** (in contrast to Business Continuity) is typically / generally ***beyond the scope*** of ***this*** guideline document. Accordingly, the below is provided for contextual & information purposes only (See **ISO 22313:2020** - clause **8.4.5** [about half a page] for further information)

In reality there is unlikely to be a formal BRP (or 'documented procedures' using 8.4.5 terminology) in the accepted sense of the word as, at this point (i.e. the point where the BRP is expected to be invoked), the ***original disruption*** event should have already been dealt with and continuity (where required) resumed / maintained at the desired level(s) (MBCO) and within the required timescale (RTO) - and the 'business continuity' team subsequently / eventually / gradually stood down as the 'business recovery' operation 'takes over'

From that point on it is more than likely that '***normal management / business***' type techniques (together with associated *normal* business resources & routines available to the organisation) will permit adequate return (recovery) to normal levels of business. However, do note that the use of some / all resources which were originally assigned to the emergency / crisis response and / or the BC response (including manpower) can still be utilised - if so required

To put 'business recovery' into some context here, the recovery time can range from very quick (e.g. minutes to hours in the case of restoring ICT type disruption) to many months or even longer (e.g. complete demolition and rebuilding of a major facility - such as a large building)

> To quote clause 8.4.5 '......................*A decision on how best to return to 'business as usual' will depend on the severity of the damage caused by the incident and estimates of how long it might take to establish the necessary facilities. The documented procedures should provide for a detailed assessment of the situation and its impact and the determination of tasks and steps required for recovery*...................'

The documented procedures for recovery should include provision for the resumption of all 'disrupted' activities i.e. not just those identified as 'key / prioritised'

This latter recognises that activities with a lower priority (than 'key / prioritised' etc. - thus having been selected for 'no action required' in the understanding the organisation' task) will also need to be resumed at some point in time, have the resource requirements so to do etc.

Maintaining the BCP

The BCP is made up of many components - some of which can be subject to rapid, regular and recurring change. If such changes are not identified and 'fed back in' to the BCP, as corrections / updates / revisions etc. - the plan could (will) quickly become worthless. Some examples of 'components' subject to change and, therefore, subject to regular review and maintenance include:

- People e.g. leaving, joining, promotion, changing role, contact information etc.
- Other stakeholder / interested party changes e.g. supplier / customer changes, regulatory changes etc.
- Changes to the basic organisation e.g. up / downsizing, mergers, acquisitions etc.
- Changes within the organisation e.g. new key services / products / activities
- Results and associated consequences of BCMS reviews
- Technology - especially ICT changes / threats / latest developments etc.
- Changes to 'environments' within which the organisation operates e.g. political
- Changes to 'locations' within which the organisation operates e.g. geographical
- Best practice - and so on ……………………………………

The deterioration time can be rapid - and what might be a very good BCP 'today', might not be fit for purpose in 6 to 12 months, if not adequately reviewed and maintained. Accordingly, the BCP (or some other associated document) must include appropriate procedures to:

1. Devise a 'system' which will find / identify relevant changes effectively, efficiently and expediently
2. Notify the changes to those 'who need to know'
3. Action / oversee the changes (whatever type of action / oversight is required)
4. Receive confirmation that change(s) has / have been effectively and adequately accounted for / addressed by all concerned
5. Update appropriate documentation / data
6. Where the circumstances of a 'change' so require, implement an associated training and / or information and / or exercise programme
7. Comply with any other 'change management' procedures if so required
8. Run an audit programme concerning 'change'

Where changes are significant, it might be necessary to go through the 'understanding the organisation' task and similar / associated processes again - and to further update the appropriate part(s) of the BCP if required, as based on the results

Deliberately Blank

Section 5 / **5** - **DO** - DEVELOPING and IMPLEMENTING the BCMS

Exercising the BCMS

ISO 22313:2020 / OPERATION / **Exercise Programme** - 8.5

Note - the words 'exercise / exercising' & 'test / testing' (as used in ***this*** Section 5 / **5**) may be regarded as being synonymous

The building blocks for planning and implementing a BCMS have already been covered in previous sections of this guideline. Whilst it might now be tempting to sit back and await an actual disruption to see how well a job has been done (or otherwise!) all of the time and effort put into the BCMS would have been wasted if, when 'tested' for real, it was found to be wanting (because it had not been adequately and sufficiently exercised)

Exercising the BCMS

Regular exercising of the BCMS is just as important as training, regular maintenance etc. The primary purposes of exercising are to:

- Provide reasonably realistic role play tools and scenarios to selected ***persons*** involved in the BCMS - in order that they are exposed to their BC roles and responsibilities etc. in ***a relatively non-threatening environment - but one which is, nonetheless, conducive to the learning, retention and experience process***

  This is accomplished via the regular scheduling of a series of different types of exercise - ranging in objectives, complexity and the requirement for associated resources

- Develop teamwork, competency, confidence, knowledge and experience amongst participants

- Verify the validity and 'usefulness' of the ***plans, procedures and processes etc.*** - which form the basis of the BCMS / BCP

- Test / validate ***technology, facilities, premises, equipment*** and other (non-human) ***resources*** etc. - as would be used for real in a major BC response

Exercising is just about the end of the line as far as practicalities of a BCMS are concerned i.e. it forms the ultimate proof (other than a real disruption response) of how well the BCMS practically performs in relatively realistic circumstances

However, some pre-requisites need to be met before exercising can take place:

- Unequivocal top management approval shall be given for the exercise to take place and for everything else listed below 'to happen'

- All BCMS documentation to be used in the exercise (plans, processes, checklists, terms of reference etc.) to be complete, up to date, fit for purpose and available to exercise participants - at least 2 months before exercise scheduled date

- All non-human resources (internal and external as appropriate) to be used in the exercise shall be available, functional and 'fit for purpose' - at least 1 month before exercise scheduled date

- All human resources (internal and external as appropriate) to be used in the exercise shall be available - both for the exercise itself and for any associated pre-exercise refresher training (the latter ideally being provided sometime during the month before scheduled exercise date)

- All appropriate feedback from previous exercises should have been responded to and the appropriate areas of concern rectified (corrected / resolved) - at least 1 month before the scheduled exercise date

- Appropriate initial and / or refresher BCMS training takes place during the month or so before scheduled exercise date

- Adequate pre-exercise warning, briefing & direction (including identification of exercise objectives and outline of the exercise scenario) is provided in adequate timeframes

- A comprehensive 'master' exercise plan is produced and generally followed to get the most out of the exercise i.e. to achieve exercise objectives. The organisation's BC Manager is typically responsible for producing same and 'managing' it 'on the day'

- Adequate exercise objectives should be set and changed regularly to ensure that over a series of different exercises (as part of an ever on-going process) the whole of the BCMS is eventually covered. (Note - for medium to large sized organisations it is highly ***undesirable*** to exercise a complete BCMS in one go)

- The planned scale, complexity & objectives (and thus impact) of the exercise should be within the BCMS scope and should ***in itself*** not be the cause of an unacceptable level of ***actual*** disruption to the organisation

The frequency & types of exercises scheduled will be largely dictated by the size / complexity / nature of the organisation. For medium to large sized organisations a major exercise should typically take place annually to two yearly - with intermediate (modular exercises) in between.

A significant change in the organisation may also trigger the scheduling of an exercise in order to validate any significantly revised BC arrangements

Whatever is decided, a suitable exercise programme should be approved (by TM) and published - typically at least ***one year*** in advance of scheduled exercise dates (there is good reason for this - but same is not expanded upon herein). Where possible, manageable, desirable and 'acceptable' - there might be merit in calling the occasional (e.g. one in every 4 to 5 major exercises) 'unannounced / no notice' exercise

Note - whilst no notice exercises obviously reflect reality and are thus desirable in one context - their use must not be abused as they can cause a withdrawal of 'goodwill' amongst volunteers (from the organisation) involved in BC planning and response

The degree of planning for a ***major*** exercise related to a ***large and complex*** organisation should not be underestimated - typically requiring anything from 6 to 12 months in total

A limitation here might be the large number of persons to be exercised (e.g. exceeding the capacity of an annual, major exercise due size of premises constraints; due taking too many staff off their primary duties at the same time etc.). This might mean that just ***one*** annual (major) exercise will ***not*** be sufficient to exercise all such personnel - without perhaps an unacceptably large 'exercise gap' (minimum two years) occurring

A proposed solution to the above problem might be to hold the '***same scenario***' major exercise every six months (circumstances permitting) - but using different exercise responders / participants for each such exercise - and then repeating the pattern 'ad infinitum' (remembering of course to change the basic exercise scenario and objectives every 12 months)

The exercise programme should consider the roles of all parties, including key third party / external providers, suppliers and others who would be expected to participate in actual / real continuity activities. An organisation may include such parties in its BCMS exercises and may also participate in ***their*** BC related exercises

Further to the above, consideration should be given to inviting appropriate (external) stakeholders / other interested parties to 'observe' exercises - typically 2 to 5 observers per exercise, circumstances permitting

An appropriately experienced & knowledgeable person should be appointed as the 'exercise director'. This will usually be the organisation's 'expert' BC person (BC Manager)

Exercises should be monitored by 'neutral' and appropriately experienced & knowledgeable persons - typically termed 'umpires'. Not only can they assist in the successful execution of the exercise but their critical feedback post-exercise can be invaluable

The culmination of every exercise is feedback i.e. what went right; what went wrong; what can we do better next time etc. Ideally, a 'hot' feedback debrief should be held immediately (for all involved) following the exercise - and the feedback documented

Within the week or so following the exercise, 'cold' feedback should be obtained to augment information gathered during the hot feedback. Cold feedback is usually obtained via documented and comprehensive reports from each exercise unit and / or participant. Where several participants from the same department or group are providing feedback - a consolidated report should be submitted. Workshops and individual consultations can additionally be used to obtain cold feedback

The results of all feedback should be co-ordinated, consolidated and collated (usually by the organisation's BC Manager or equivalent person) and recommended remedial action points, corrective action allocations (to appropriate persons) and 'completion' timescales produced

The above is then combined with an overview post-exercise report, which is submitted to top management for review and sign-off - the latter being the authority for corrective action points etc. to be addressed as required (including any associated budget requirements)

All corrective action points (including the provision of extra resources, budget etc. - where so required) should be satisfactorily resolved at least 1 month prior to the scheduled date of the ***next*** major exercise. Any associated budget and resource issues should also be satisfactorily resolved by this point

Note - similar feedback considerations and resolutions will also apply of course - following any BC response to ***real*** disruptions

Final Word

Remember - any BCMS will be 'worthless' unless it is ***adequately trained AND exercised*** on a reasonably ***regular basis***

Note: - The detailed plans, procedures and processes necessary to conduct BCMS related ***exercises*** are (with the exception of what has already been documented above) ***beyond the scope*** of this guideline

It is strongly recommended that the user / reader studies all of ISO 22313:2020, clause 8.5 - with particular emphasis on clause ***8.5.3***

ISO 22313:2020 / OPERATION / **Evaluation of BC Documentation & Capabilities** - 8.6

Note to Reader / User:

Clause 8.6 was originally 'clause 9.1.2' in the ISO 22313:20**12** inaugural version

As the subject of 'evaluation' should logically be covered in **Clause 9** of ISO 22313 under title 'Performance Evaluation' - one wonders why ISO chose to place it in Clause 8 (specifically clause 8.6) in the 2020 version (even if the subject matter relates to 'BC Documentation and Capabilities')

It is suggested that if an organisation is considering ***aligning*** its BCP with ISO 22313:2020 - then anything which appears in the latter's clause 8.6 might be amalgamated with / merged into clause 9 instead (but only to the extent that clause 8.6 info is ***not already adequately covered*** by said clause 9)

However, if the intent is to ***certify*** a BCP to ISO 22301:2019 - more care will be required in how clause 8.6 of ISO 22313:2020 is to be 'managed' (Note that there is no clause 8.6 in ISO 22301:2019 itself)

Either way, the 'serious' reader might wish to take a look at clause 8.6 - which will, of course mean having access to ISO 22313:2020 (however that might be accomplished [hopefully without the need to purchase it!])

Deliberately Blank

Section **6 / 1**

Check & Act

BCMS Performance Evaluation

Cross Reference - ISO 22313 / **Performance Evaluation** - 9

We are now into the final two elements of the ***PDCA*** Cycle i.e. '***CHECK*** and ***ACT***' ……………………………

In order to demonstrate on-going:

- Conformity of the BCMS (to whatever it is required to conform with)
- Adequacy of the BCMS (the BCMC is 'fit for its intended purpose ')
- Continual improvement of BCMS effectiveness and efficiency etc.
- Continual improvement of BCMS customer satisfaction

………………… the organisation's BC Manager (or otherwise the most appropriate person in the organisation) should originate, plan for, document, resource, implement, maintain, review and improve the various monitoring, measurement, analysis & evaluation procedures needed to establish and demonstrate the BCMS 'conformity', 'adequacy' and 'continual improvement' (performance & effectiveness) requirements referred to a little further above

Such 'procedures' should be applied on a regular, systematic and on-going basis

Monitoring, Measurement, Analysis & Evaluation - **MMA&E** (of the BCMS) (ISO 22313 - 9.1)

The above mentioned procedures etc. should adequately account for:

- The 'rules' whereby MMA&E are deployed / employed e.g. what is to be monitored / measured + when, how and by whom + how are the results analysed / evaluated etc.

- Relevant / pertinent and available ***historical information*** deemed to be 'still useful etc.' regarding any particular 'performance evaluation' context under consideration

- Setting of ***performance indicators*** (including qualitative / quantitative *measurements*) appropriate to both the needs of the organisation and achievement of valid results

Note: - ***Performance indicators*** / ***metrics*** (e.g. management, operational and economic parameters) are basically ***evaluations*** which ***measure*** both ***conformity*** with and ***improvement*** of the BCMS and its outcomes. They should also provide the information necessary to identify success and / or those areas requiring correction and / or improvement

- ***Monitoring*** the extent to which the organisation's business continuity policy, objectives, targets, strategies, tactical outcomes etc. are being met

- ***Evaluating*** the performance of the BC measures put in place to ensure the continuity of key (prioritised) products, services, operations, activities and processes etc.

- ***Monitoring*** pro-active compliance of the BCMS with applicable legislative / statutory, regulatory and similar requirements

- Reactive measures to ***monitor*** failures, incidents, non-conformances (including near misses and false alarms) and any other evidence of deficient BCMS performance

- ***Recording*** data + ***analysing*** results of ***monitoring*** & ***measurement*** activities - sufficient to facilitate the identification of the subsequent ***corrective action****(s)* required

- Providing, retaining and maintaining associated reports, records and other required documentation (collectively known in the MMA&E context as '*evidence*')

Use of the word 'evaluation' in the ultimate BC sense typically relates to the concept of '***continual improvement***' with regards to '***customer satisfaction***' - whoever and in whatever context the customer might be identified (See also Section 6 / 2 of this guideline document)

Note: - The term 'customers' as used herein refers to 'stakeholders / other interested parties' having e.g. some interest(s) of '***value***' (tangible and / or intangible) in / re the organisation. Some examples of BCMS customers can include:

- Organisation's staff / employees
- Recipients of organisation's key product(s), service(s), operation(s) e.g. customers; hospital patients; the general public etc.
- Shareholders
- Suppliers
- Dependencies
- Legislators / Regulators

Concerning most airlines, airports etc. the most important 'customer' of all is the potential or actual traveller (i.e. passengers - but could be freight shippers for a cargo airline; duty-free concessions at airports etc.). The latter will typically be direct recipients of the adverse impacts of any ***real*** (significant), associated disruption event and will thus be a valuable feedback source related to same - and should be used as such accordingly and where feasible

Compared to the relatively simple process of e.g. evaluating on board customer service during a non-disrupted flight (typically be completing a customer satisfaction form delivered and collected by cabin staff) - obtaining critical feedback from potential and actual passengers associated with how the airline handled a ***real*** disruption event (which adversely impacted on said passengers in some significant way) will be more problematic

* However, the latter is perfectly feasible and should be implemented (despite the difficulties) - circumstances permitting. How this is accomplished is beyond the scope of this guideline

* A typical example relates to the massive disruption to many ***airlines and airports*** (and hence their customers) caused by the 2010 closure of much of N European airspace due volcanic ash. Post-disruption feedback provided by impacted customers was invaluable in 'working out' how to better handle similar impact disruptions moving forward

The organisation should strive for ***continual improvement*** of its products, services and operations by demonstrating compliance with its own BC Policy, Objectives and Strategies etc. (amongst other things) - and by use of audit, data analysis and management review

Internal Audit (ISO 22313 - 9.2)

Note 1 - The detailed methodologies of auditing are generally ***beyond the scope*** of this guideline document. However, some basic explanatory material is necessary and has been included further below. The user / reader should also refer to ISO 22313 - clause 9.2

Internal audit of the BCMS provides a mechanism for measuring the extent to which it (the BCMS) is achieving its objectives, conforming to its planned arrangements and has been properly implemented and maintained. It can also identify opportunities for improvement

Note 2 - Information provided further below on ***other*** types of audit (e.g. **external** audit) and associated material is provided for contextual purposes only i.e. same has ***not*** been covered by ISO 22313

Note 3 - Apart from 'self-assessment / operational evaluation' type audits, ***internal*** audit of the BCMS is typically ***not*** performed by the BC manager or anyone related to the BCMS in general - such as the Top Management BC Champion' or the 'BCMS Steering Committee' or any of the 'Disruption Support Units' etc. Instead, ***internal*** audits of the BCMS are typically performed by the organisation's compliance / audit business unit (or equivalent) and / or otherwise by an appropriately experienced, competent, qualified and independent external party

This section generally refers to ***audit*** (in one form or another) of the ***BCMS*** - together with the associated ***monitoring*** process - the latter being required so as to ensure that audit recommendations are adequately effected (dealt with) within the required / specified timescales and to the required / specified degrees / levels

A BCMS ***internal*** audit generally involves an impartial review of same (i.e. the BCMS), evaluated against pre-defined standards and / or policies and / or requirements etc. - together with the provision of remedial recommendations (***corrective action***) where appropriate

Such audit should be routinely conducted at least once every two years, but ideally annually or when so required e.g. by a regulatory requirement; by 'other interested parties' with good reason; when an associated 'problem' is identified etc.

*The **pre-audit** Process (i.e. not the audit itself)*

All concerned should clearly understand (beforehand) the particular type of pre-audit processes / procedures to be used for the specific audit to be undertaken - and should follow same ***prior to*** an actual audit taking place. For example, it might be necessary for the part of the organisation being audited to conduct a GAP analysis in the appropriate areas (i.e. those to be audited) before the audit is due to be conducted

(A GAP analysis provides opportunities for an organisation to identify any actual or potential deficiencies [non-conformities) in designated parts of its 'business / operation etc.'- permitting said organisation (more correctly the appropriate part[s] of the organisation) to take appropriate remedial action i.e. ***before*** the audit actually takes place)

The Audit *(described in general terms only)*

A BCMS audit (as with any 'modern management system' audit) typically covers / includes (list is not exhaustive):

- Type of audit required e.g. internal / external / self-assessment (operational evaluation); periodic; compliance; best practice etc.
- Audit objectives
- Audit scope
- How the audit is to be *conceptually* conducted (audit framework) e.g. in compliance with a standard (such as ISO 22301; in accordance with a legal / regulatory etc. requirement; in accordance with an approved BCMS document etc.
- Audit protocols to be followed e.g. notification of audit date(s) and timetables; provision of required pre-audit information to auditee(s); opening and closing briefs; complaints procedure etc.
- How the audit is to be *practically* conducted (audit approach) e.g. questionnaires; face to face interviews; inspection of documents; types of audit evidence required etc.
- Information / evidence gathering e.g. by walk through of a process; by sampling documentation; face to face interviews (again) etc.
- Compiling & collating audit documentation and similar e.g. results of questionnaires; records / reports re face to face interviews etc.
- Producing *initial* results / conclusions (findings) of the audit; reviewing these findings against the audit framework and adjusting if necessary
- Producing draft *final* findings (including recommendations) and a supporting report - followed by discussion & debriefing e.g. with appropriate stakeholders / other interested parties - and documenting the associated feedback / conclusions
- Producing ***final*** findings (sometimes with recommendations - depending on the audit scope) and the supporting report - to be presented to the original audit sponsor. The final report should identify if any unresolved 'differences of opinion' remain between auditor & auditee(s)
- Providing an agreed ***remedial action plan*** (if so required) to address the agreed recommendations of the audit (as appropriate)
- Providing a suitable ***monitoring*** (if so required) plan to ensure compliance with the agreed remedial action plan

Internal Audit Procedure *(Specific)*

Detailed internal audit procedures are described in ………………………………… (Note - this particular subject is beyond the scope of this guideline document – and thus no detail is included here)

External Audit

Reminder: Included for information and context purposes only

BC related audits (e.g. supplier ***evaluations***) conducted by the organisation on ***external*** parties (e.g.3rd party vendors supplying services to the organisation) shall be conducted by ………………………………………… in a similar manner to those stipulated for internal audits (insofar as the external party agrees)

Overview service level requirements for current 3rd party vendors are shown at …………………………………

External organisations requiring such audit are:

a. ……………………………
b. ……………………………
c. ……………………………
d. etc.

External BC related audits conducted ***on the organisation itself*** (by external / 3rd parties) shall be conducted under mutually pre-agreed procedures

Note: ***External*** audit gets only one mention in ISO 22313:2020 (see 3rd para of clause 8.6.1). Nevertheless, it is an important subject which must (in reality) be adequately addressed by the organisation - where appropriate

Additional Information - Audits

Audit Non-conformities

Monitoring, measuring & analysis (by means of audit, inspection, operational evaluation etc.) - will ensure, insofar as possible, compliance with the requirements stipulated in ………………………………

Any nonconformities identified will be recorded and communicated to the 'Responsible Manager' (person responsible for making corrections and taking corrective and / or '*preventive'* action) and, if appropriate, also to the 'Accountable Manager' (senior manager ultimately accountable for the BCMS). The Responsible Manager shall then investigate in order to establish the root cause of nonconformities - and implement the required 'correction' and / or 'corrective / preventive action'

The organisation's BC Plan should include procedures designed to ensure that appropriate & timely 'correction' and / or 'corrective / preventive actions' etc. are taken, in response to audit / inspection / operational evaluation findings and feedback. Such procedures should be designed to *monitor* these latter actions, in order to verify their effectiveness and completion in a timely manner

The Accountable Manager shall have the ultimate responsibility for ensuring correct and timely compliance by the Responsible Manager, concerning such actions as stipulated immediately above - and that the correction or corrective / preventive action taken has re-established (or will re-establish) compliance with the relevant requirement(s) etc.

Subsequent to audit / inspection / operational evaluation, where audit findings or feedback requiring action have / has been made, the following will be established by the Auditor:

- The nature and seriousness of findings and the possible need for immediate action
- The origin of the finding plus any associated objective evidence
- The details of the correction or corrective / preventive action required
- The schedule for correction or corrective / preventive action *
- The identification of the relevant Responsible Manager
- The necessity to forward the finding to the Accountable Manager *

* Managed by the appropriate 'Responsible Manager' - in conjunction with the associated auditor

Personnel Assurance Programme

Personnel 'required to manage and / or operate' the BCMS should be subject to an '***assurance programme***'. Such programme should typically (list is not exhaustive):

- Define associated 'terms of reference', accountabilities, roles & responsibilities, authorities etc.
- Define associated 'Key Performance Indicators - KPIs' e.g. objectives, standards to be met, measurement methods to use etc.
- Define factors related to the above which determine 'success'
- Include associated KPIs in employment contracts, annual appraisals etc.
- Evaluate individual's performance against the items in the 4 bullet points above (performance appraisal)
- Provide a 'personal' remedial action plan where deemed necessary

Analysis of Data

An organisation should maintain and retain appropriate documentation, including ***monitoring*** *and* ***measurement*** data, which can be ***analysed*** to demonstrate the suitability and effectiveness of said organisation's BCMS. Such documentation should also be used to assist in the ***evaluation*** process required to ensure / achieve conformity and continual improvement. A typical example might be analysis of call out (alerting / notification) records (numbers responding, times taken etc.) and recruitment / retention rates of disruption related volunteers (e.g. those providing humanitarian / welfare services as part of the IRS)

Audit feedback should be analysed to establish trends, problems, areas exhibiting continual improvement etc. The results should be considered at '***Management Review***' meetings

Corrective / Preventive Action - (See Sub-section 6 / 2 [starts page 256] of ***this*** guideline document)

Review of the BCMS

General

To remain effective, efficient and 'fit for purpose', a BCMS should be ***reviewed*** at planned intervals as specified in the BC Policy + whenever significant change occurs in the way the associated organisation operates

There are several methods of reviewing the BCMS, one of which includes a formal 'audit process' of one kind or another - and this has already been referred to above. Examples of reviews ***not*** involving the formal audit process typically involve self-assessment - and include:

- Post-exercise reports
- Modular reviews of BCMS - typically performed by organisation's BC Manager / equivalent person
- Full reviews of the BCMS - typically performed by the *top management's* BC working group - in conjunction with the BC Manager. Alternatively, such review functions may be outsourced to an appropriate specialist(s)

The purpose of any review (formal audit or otherwise) is to demonstrate that the current BCMS is fit for purpose and to further identify opportunities to continually improve same, with the ultimate aim of improving customer satisfaction - whoever the customer might be

Full / Major reviews of the BCMS should (when completed) be presented to TM for approval and sign-off - which effectively endorses the BCMS until the next major review is accomplished

All appropriate, associated documentation should be maintained and retained (as required) in order to reflect the approved outcomes of reviews

Reminder: the 'serious / interested' should also take a look at ISO 22313:2020 - clause 9.2. For further info re audit of (modern) 'management systems' refer to (separate document) ISO 19011:2018. An 'unofficial' version [(use with caution] of ISO 19011:2018 can be found by following the below link:

https://www.bahamas.gov.bs/wps/wcm/connect/831eff20-6617-4ef8-be28-685c308948ed/FDBNS+-+Guidelines+for+Auditing+MS.pdf?MOD=AJPERES

Management Review (ISO 22301 clause 9.3)

TM review / appraisal (of the BCMS) can be used to evaluate the ongoing suitability, adequacy, effectiveness & efficiency of same - and should encompass (list is not exhaustive and is in approximate order corresponding to how a 'typical' BCMS is produced / documented etc.):

- Policy, objectives, scope, exclusions etc.
- Risk acceptance / appetite
- The various components falling under 'Understanding the Organisation'
- BC Strategies & associated BC Tactical Treatments / Solutions etc.
- The IRS + BC plans & procedures etc.
- Awareness, Competence and Exercising
- Communications

- Documentation
- Maintenance
- Performance Evaluation (including trends apparent from non-conformities, corrective actions etc; the results of monitoring, measurement, audit findings etc.)
- Continual Improvement opportunities

Other considerations include (again, list is not exhaustive):

- The status of actions from previous management reviews
- The effectiveness of supply chain continuity arrangements (as appropriate)
- Changes to the organisation and its context
- Relevant feedback from stakeholders / other interested parties

The ‘management review’ typically takes place over a period of time (i.e. ‘not all at once’) and should be scheduled and documented accordingly. Persons who are significantly involved in ‘managing’ the BCMS should be co-opted / involved - as appropriate

The following may trigger an ‘ad hoc’ management review and should otherwise be examined / assessed (anyway) in preparation for scheduled reviews (list is far from being exhaustive):

- Associated and appropriate sector / industry trends
- Legal and / or Regulatory changes
- Actual BC incident experience, feedback etc.
- Disruptions affecting other organisations in a similar type of operation etc.

For example purposes only, outputs from management review might result in the following changes to the BCMS (list is far from being exhaustive):

- Variations to the scope
- The need to revisit the ‘understanding the organisation’ task
- Updates to business continuity strategies and associated tactical treatments / solutions
- The need to rewrite BC Plans etc.

The organisation should:

- Take appropriate action relating to these results / outputs of management reviews
- Communicate said results to appropriate stakeholders / other interested parties
- Retain appropriate documented information as associated evidence of ‘what has been done and achieved’ during any particular management review

Section **6 / 2**

Check & Act

Continual Improvement of the BCMS

Cross Reference - ISO 22313 / **Improvement** - 10

Non-conformity and Corrective Action (ISO 22313 - Clause 10.1)

Note - Detailed methodologies of ‘Non-conformity’ & associated ‘Corrective / Preventive Action’ are generally ***beyond the scope*** of this guideline document. However, some explanatory material is necessary and is included below. The user / reader is advised to also refer to ISO 22313 - clause 10

- **Non-conformity** = Non-fulfilment of a requirement

The organisation should determine opportunities for improving the BCMS and then implement the associated actions necessary to achieve same ………………. e.g. by identifying causes of non-conformities (actual and potential), controlling, containing and correcting them; dealing with their consequences; evaluating options to eliminate said causes and then eliminating them etc.

Non-conformity *+ associated* ***Corrective*** *and / or* ***Preventive Action***

The findings of audits, feedback reports etc. typically identify at least some ‘non-conformities’. If so, preparation and implementation of timely ***corrective*** and / or ***preventive*** actions (which are ***respectively*** designed to ***correct*** 1: - any ***existing*** non-conformities found and deal with their consequences ………….. and 2: - to identify and ***prevent potential*** non-conformities ***before*** they can occur) will be required. A third categorisation might be made - i.e. an ‘***observation***’

In most aviation related organisations (e.g. airlines, airports, ground handlers, maintenance & repair organisations etc.) the subject of ‘non-conformity and corrective action’ is typically not managed by anyone who is part of the organisation’s BC business unit - even if the latter exists!!! (The organisation’s ***compliance*** / ***audit*** business unit [or equivalent e.g. flight safety business unit; quality business unit etc.] typically assumes this responsibility)

Corrective Action - is taken to eliminate the root cause(s) of identified, ***ACTUAL*** non- conformities in order to prevent re-occurrence. Top management should ensure that corrective actions are implemented in a timely manner and that there is systematic follow-up to evaluate the effectiveness of such actions. A typical (associated) process comprises:

- Identify non-conformities
- Determine root cause(s) of non-conformities
- Evaluate various remedial action plans for removing non-conformities
- Choose and implement the most appropriate remedial action plan(s) - otherwise known as ‘corrective action(s)’
- Document all of the above
- Review (monitor / follow-up) any corrective actions taken

Preventive Action - is taken to eliminate the root cause(s) of identified, ***POTENTIAL*** non-conformities ***BEFORE*** they can occur. A typical process comprises:

- Identify ***potential*** non-conformities
- Determine cause(s) of potential non-conformities
- Evaluate various remedial action plan(s) to remove potential non-conformity causes
- Choose and implement the most appropriate remedial action plan(s) - otherwise known as 'preventive action'
- Document all of the above
- Review (monitor) any preventive actions taken

Establishing procedures for identifying and addressing actual / potential non-conformities + the taking of appropriate corrective and preventive actions respectively (on an ongoing basis), assists with the reliability and effectiveness of an associated BCMS

Such procedures should define the responsibilities / authorities / actions etc. to be taken in planning and implementing same. TM should ensure that such actions are accomplished and that there is systematic follow-up to evaluate their effectiveness

Associated documented information should be retained

Continual Improvement (ISO 22313 - Clause 10.2)

See also 'Customer Satisfaction (Continual Improvement)' related text - page 249

In the context of BCMS continual improvement (e.g. suitability, adequacy, effectiveness etc. at all levels within the ***PDCA*** Cycle) matters should be driven by e.g. BCMS policy, objectives, audit results, disruption analyses, management review, future development etc.

An associated process should be developed which identifies associated opportunities (for improvement) and manages them. Said process might be based on that used for * corrective & preventive action etc. and could e.g. include (very simplistically) the following:

- Identify what to address i.e. whatever is under consideration + its current 'condition'
- Identify the present (continual improvement) process and controls (if any) in place
- Determine the 'improvement' changes required and implement same

* Corrective / preventive actions address deficiencies in the BCMS and ensure that it functions as intended, while continual improvement takes the BCMS to a higher level of efficiency and effectiveness

Note: The organisation can achieve improvement via effective application of BCMS processes e.g. leadership, planning, performance evaluation etc. Opportunities can also arise from changes in e.g.

- Context of the organisation (e.g. failure of a competitor; re-locate to a better environment etc.)
- Organisation's internal structure (e.g. via acquisition of additional locations, staff etc.)
- Means of production, delivery etc. (e.g. technological change, infrastructure improvement)
- Evolving BCMS methodologies, new recovery methods etc.
- Technology and associated practices, including new (particularly ICT type) tools and techniques

Sub-section 7

CONCLUSION

The various environments and contexts (political, legal & regulatory, commercial, instant communications, financial, customer / client awareness & intolerance, environmental, geographical, illegal etc.) in which large and medium sized organisations (including airlines, airports etc.) operate today, no longer permit them to ignore (without some degree or other of risk to the organisation) the consequences of not having adequately planned for and resourced for responding to the appropriate threats (and thus potential disruption) potentially facing them

The expectation of the 'modern world' today is that such plans and resources ***must*** be in place. If they are not (and / or are inadequate), the risk to an organisation emerging from a major disruption event - without damage to its reputation and / or 'financial bottom line' are significant - possibly to the extent of ceasing operations - possibly permanently

Furthermore, governments, regulators, customers & similar stakeholders / interested parties etc. are increasingly '***holding an organisation's top management and specialists to PERSONAL account***' for any negligent etc. pre-preparation and / or actual handling of / response to a crisis - including any with significant ***Business Continuity*** (Disruption) connotations

This can practically mean imprisonment and / or the imposition of very substantial fines (feasibly running into tens of millions of dollars - and possibly much more - just think of the BP oil spill in the Gulf of Mexico!):

> Quote '……………………….**BP is responsible for close to $40 billion in fines, clean-up costs and settlements - as a result of the oil spill in 2010 - with an additional $16 billion due to the Clean Water Act**……………………'

Because the 'unexpected' ***will*** eventually occur, organisations should (without delay) adopt modern management 'tools' to assist in the desired response - one of which is the implementation of a fit for purpose ***Business Continuity Management System***

Airlines, Airports, GHAs etc. are no exception to the above

Deliberately Blank

APPENDIX A

CASE STUDIES

Case Study **1** (based on real events in the Middle East in early 2003)

A brief overview

DISRUPTION to *'ABCX Airways'* AIRLINE OPERATIONS (Due potential military operations in IRAQ - which eventually materialised as the second Gulf [Iraq] War - commencing March 2003)

Note: For the purposes of this case study the user / reader can assume that *'ABCX Airways'* is a major Middle East scheduled passenger airline headquartered at its main hub airport in the Arabian Gulf region - located to the south-east of IRAQ and to the south of IRAN. The circumstances were real, as is the document below (i.e. as it was *originally* produced) - which provided a *briefing overview* to senior managers as to how the airline was preparing itself to handle potential disruption, should hostilities break out. The identity of the airline and some other minor details have been changed

Roles, Responsibilities & Manning of the Disruption Planning Unit (DPU), the Flight Disruption Co-ordination Centre (FDCC) and Disruption Support Units (DSUs)

Introduction

1. Disruption to *'ABCX Airways'* operations may be caused by many factors, the more usual being poor weather and / or runway closure; aircraft (fleet) grounding; an aircraft emergency and / or accident; industrial action etc.

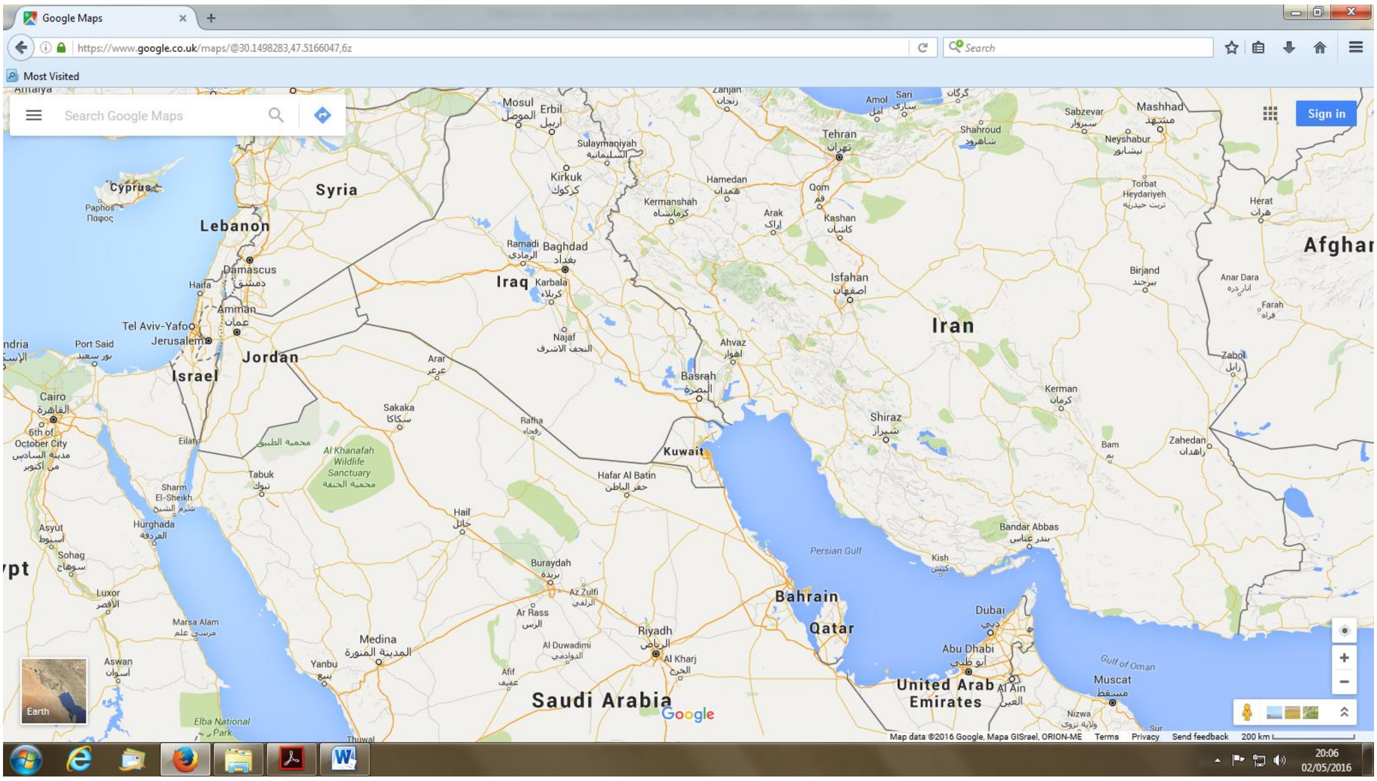
   ABCX Airways is currently (January 2003) preparing for a potential major *disruption* should military action commence in nearby Iraq in the near future - such military action having the potential for serious to severe (adverse) operational and commercial disruption impact on airline operations

2. The detailed and already approved "Iraq Disruption Plan" (separate document - not included here) has been prepared by the airline's Crisis Response Planning Department and presented to a variety of audiences, including ABCX Airways top management and the *'XXX'* Civil Aviation Authority

3. The role of the Crisis Response Planning Department is to now liaise and co-ordinate with all airline departments / individual business units which potentially have a disruption response role to play - in order to transform the paper plan into one which will work 'on the day'

4. Lessons learned from previous major disruption events indicate that the current ABCX Airways 24H Operations Control Centre (OCC) infrastructure would not be capable of adequately supporting the demands of the necessary and additional (disruption related) direction, co-ordination, information (flow) and support responsibilities required - in addition to its 'normal business' roles & responsibilities

Accordingly, the 'Iraq Disruption Plan' should enable the OCC and Disruption Planning Unit (DPU) to focus on ***strategic*** disruption planning and response - whilst the Flight Disruption Co-ordination Centre (FDCC) and Disruption Support Units (**DSUs**) co-ordinate and implement plans, resources and logistics at the ***tactical*** level - as based on DPU produced strategy



Plan Outline

5. The Disruption Plan is based on:

a. *Assessment of Impact of Disruption*

- The OCC will initially categorise the anticipated disruption impact as "Minor, Medium or Major"

- *Minor* disruption (minor adverse impact) would be handled by the airline's 'normal operations' day to day working system and manning

- *Medium* disruption(serious adverse impact) will require extra assistance to resolve, requiring activation of the DPU - the latter operating from the OCC

- *Major* disruption (severe adverse impact) would require activation of the DPU (operating from the OCC) together with the FDCC - the latter operating remotely from the OCC

- It is anticipated that initial disruption as a consequence of Iraq hostilities will be classified as "Major

b. *Effective Utilisation of DPU and FDCC*

With the DPU and FDCC operational the Company is expected to be able to maintain a degree (unspecified) of concurrent normal and major disruption operations provided appropriate airspace remains available for flight operations

DPU (Operational for both *Medium* & *Major* Disruption)

6. The role of the DPU is to make the ***strategic*** decisions necessary to manage and bring the disruption to a successful conclusion

7. The DPU will be manned 24H by senior staff (strategic decision makers - GM / VP or above) from appropriate ABCX Airways departments. Other senior staff (including the airline's top management) may be co-opted by the DPU - as required by the situation 'on the day'

   All DPU designated personnel shall be familiar with their disruption roles and responsibilities and will operate from the DPU room located adjacent to the on-duty OCC Manager's desk

FDCC (Manned for Major Disruption Only)

8. The FDCC facilitates the ***tactical*** execution of DPU strategic decisions

9. The FDCC is manned (from a centralised and appropriately equipped operating location) by personnel from various departments / business units having a disruption response role to play. For an operational type disruption (e.g. affecting flight operations) the FDCC will typically be manned by personnel from:

   - Aircraft Engineering / Maintenance
   - Airline Planning
   - Airport Services (Hub)
   - Airport Services (Outstations)
   - Cargo
   - Commercial (representing Marketing, Retail, Ecommerce etc.)

- Corporate Communications / PR (External & Internal & website)
- Customer Services (including In-flight Services [Cabin Crew] & normal ops call / contact centres)
- Emergency (telephone) Call / Contact Centre
- Flight Operations
- Holidays & Tours (Leisure) etc.
- In-flight Catering
- IT & Telecommunications
- OCC representation - including crewing
- Revenue Optimisation / Yield Management
- Safety
- Security
- Special (Humanitarian) Assistance Team
- Transport & Accommodation Services
- ……………………. anyone else required ‘on the day

Other Departments may be asked to provide staff as required by the disruption circumstances (e.g. Industry Travel; Procurement & Logistics; Legal; Finance; Insurance, HR etc.)

The FDCC will be led by an appropriately trained and exercised senior managers (General Manager / Vice President / equivalent) having appropriate background and experience

10. The FDCC must be capable of being shift manned 24H for as long as is required

11. Personnel manning FDCC positions will do so from ‘spare’ helpdesks located in the ABCX Airways Emergency Telephone Call Centre. All disruption calls not directly the responsibility of the OCC / DPU will be routed to the FDCC via telephone Filter Desk operators located in the OCC. The role of the Filter Desk is to direct the disruption call to the appropriate FDCC helpdesk

Disruption Support Units (DSU)

12. DSUs essentially comprise assigned personnel from individual airline departments / business units - having a disruption response role to play. Department / business unit managers will split their staff with ***one part of the split dealing directly with disruption issues*** whilst the ***other part maintains concurrent normal operations insofar as is possible.*** 24H operations (shifts) should be planned for

    DSUs can operate from either the FDCC and / or from their *normal work locations* - as directed e.g. HR personnel will not normally be required to operate from the FDCC. However, HR *will* generally have some disruption roles to play, and these would be carried out by selected HR staff (i.e. provided by the HR DSU) operating from their normal work locations

Individual Departments / Business Units having FDCC Roles

13. At time of writing, the FDCC role / manning is essentially a new concept (as is the DPU) and has not yet been utilised in the full manner described above. However, the concept is considered sound and appropriate department heads / key players (for those departments / business units required to contribute to the manning of the FDCC) are now asked to carefully consider the following and act accordingly:

    a. Department Heads will decide if their units might have a disruption role to play (with associated advice and ongoing support being provided by the Crisis Response Planning department)

    b. If a disruption role is identified, an agreed portion of department / business unit personnel shall be pre-allocated to form the department / business unit DSU

    c. Depending on the nature of the contingency (again, in this case, Iraq) the specific disruption roles and responsibilities of each DSU shall be decided

    d. Once c. above has been resolved, appropriate procedures / checklists etc. should be produced / documented and DSU staff pre-briefed / pre-trained as necessary (with advice, support and training being provided by the Crisis Response Planning department)

    e. Department Heads should decide whether activation of their particular DSUs (at little or no notice) might be necessary at time of major disruption. If so, the necessary pre-arrangements for this to be accomplished shall be made

    f. DSU activation will be initially invoked by the OCC depending on circumstances i.e. certain DSUs will always be activated for major disruption. Other DSUs will be activated on an "as required" basis, depending on the nature of the disruption

    g. DSUs will operate from either the FDCC and / or normal work locations – as per SOPs or as directed

14. IT support will be contacting all DPU / FDCC liable departments / business units / individual staff, with a view to discussing and implementing the various IT systems, applications, network accesses and telecommunications required when operating from DPU or FDCC workstations

15. Notwithstanding the potential Iraq disruption, this plan (modified as necessary) will be activated in future to deal with ***any*** significant disruption related event. The objectives, first and foremost, are to protect the interests of our customers and minimise the impact of disruption thereupon. Success in this area will also help to protect the reputation of our airline and minimise any threat to future business

16. Crisis Response Planning Department is here to assist all personnel involved in making the above plan a working reality. Please do not hesitate to contact us if required

    The “reality” of what has been documented above should be in place, and ready to go, by no later than end of January 2003 - as agreed to by airline top management

Note: Above prepared by ABCX Airways Crisis Response Planning Department - 20 Jan 2003

Deliberately Blank

Case Study **2** (based on real events in the UK in 2005)

BA - Catering Strike + Consequential Industrial Action by LHR Baggage Workers / August 2005

A brief overview

On 10 August 2005 Gate Gourmet (sole supplier to British Airways [BA] of in-flight catering at London Heathrow airport [LHR]) was adversely impacted by unofficial industrial action taken by its own (Gate Gourmet) staff

The next day around 1000 BA staff at LHR (mainly baggage handlers and loaders) also stopped work in 'sympathy' with the involved Gate Gourmet staff. By that evening all BA flights from Heathrow were cancelled due lack of catering and baggage services - involving more than 100 flights and around 15,000 stranded passengers

Over the next two days BA was forced to cancel hundreds more flights from LHR and strand 85,000 more passengers - as the 'unauthorised' industrial action by its staff continued. Even when these BA staff resumed normal work duties, the on-going Gate Gourmet dispute meant many flights departing LHR without catering

The eventual result for BA was sharp criticism from many of its stakeholders (especially customers) and an estimated loss of GBP £45 million. The adverse impact on its reputation and image was probably equally severe

How might a robust BC Plan have mitigated the above adverse consequences?

- Firstly, Gate Gourmet was a critical supplier to BA at LHR. ***A sound BC Plan would have pre-identified this criticality*** *(risk / threat)* ***and demanded an acceptable and appropriate solution option*** - to be approved by senior BA management, documented, resourced, trained for and exercised

  The starkly obvious solution options (BC ***tactical treatments***) might have been to:

  - Use more than one in-flight catering supplier at LHR
  - Have contingency plans in place to transport catering into LHR from other nearby airports not affected by industrial action (e.g. London Gatwick - LGW, London Stansted - STN and London Luton - LTN)
  - Departing flights from LHR could have been planned to briefly land at the latter (above) airports, load the catering and then depart for scheduled destination - with minimal delay to normal schedule - albeit incurring additional costs in so doing (1. but nowhere near £45 million) 2. (runway and en-route slots are obviously a major consideration if this option was to be implemented)

- *'If the probability and estimated adverse impacts of potential industrial action by staff within an organisation are judged to be significant - then an appropriate BC solution option should be planned for ………………………………………….'*

  Concerning the BA baggage handlers' industrial action - a typical BC option (tactical treatment) here might have been to cross-train other *appropriate* staff within the organisation (typically junior and mid-level managers) to conduct the duties of those staff prone to industrial action (accepting that there will still be manpower shortages)

  Another option might have been to charter, lease or buy-in appropriately skilled and trained staff from third party suppliers (e.g. ground handling operators) - not necessarily UK based. Further options might have included directing and / or transporting passengers to other appropriate airports where BA had a 'non-striking' presence - or to other airlines at LHR serving (at least many of) the same destinations as BA (provided, of course, that the baggage handlers servicing such airlines were not the same as those used by BA)

- *Stakeholder / other interested party communication must be an immediate priority for the organisation - particularly with customers and the media*

  If used effectively, efficiently and quickly - traditional and social media comms can be used to *pre-inform* and / or update many customers of an actual or potential problem. If this is done successfully the disruption and frustration to customers can be minimised, as can the associated adverse impacts on the airline. Examples of communication methods include telephone, email, text message, website, social media etc. The media (press, radio, TV etc.) can also be used to convey information

- *Logistical BC planning for the lack of in-flight catering from a sole, critical supplier should include alternative methods of customers being able to obtain catering locally*

  For example, distribution of vouchers to customers on check-in, with which they could purchase catering of choice for their journey from airport concessions (shops). The 'cash equivalent' of the voucher should be adequate for its purpose (it is possible that this was not the case in the above BA situation) and a pre-planned procedure invoked to ensure that concessions do not run out of supplies (as happened at LHR [i.e. actually ran out of stock)

  Another option might be to communicate with customers *before* they report to the airport - to advise them of the problem and to bring their own catering with them. A suitable form of 'compensation' could then be offered at check-in e.g. cash, discounts on future travel etc. The security restrictions on 'liquids' to carry-on to the flight could be overcome by providing airside vouchers with which to purchase carry-on drinks

http://www.thisismoney.co.uk/news/article.html?in_article_id=404808&in_page_id=2

Deliberately Blank

Case Study **3** (based on real events in the UK in 2008)

LHR - 'New' **Terminal 5 Crisis** (BA & BAA) - March 2008

A brief overview

On 27 March 2008 British Airways (BA) opened its new Terminal 5 at London's Heathrow Airport (LHR) - which immediately ran into massive problems resulting in what might be termed 'a major public relations and customer service disaster'. To quote from one UK newspaper the following day:

' .... The chaotic scenes as the new Terminal 5 at Heathrow opened yesterday were a classic example of a British public relations cock-up!

Instead of being met with a high-tech, hassle-free travel experience, passengers were faced with overcrowding, delays, cancellations, ill-trained staff and baggage chaos

British Airways - which has exclusive use of the terminal - was forced to warn passengers that one in five flights from Heathrow's Terminal 5 were likely to be cancelled today after it struggled to rectify yesterday's operational nightmare. It is a major embarrassment for BA, airport operator BAA and the UK Government, which have all hailed the Lord Rogers-designed building as state-of-the-art ....'

Terminal 5 was publicised as 'one of the most technologically advanced airport terminals in the world' - but British MPs (Members of the UK Parliament) subsequently described its opening as a "national humiliation"

During the first five days of the Terminal 5 operation, BA is reported to have misplaced more than 23,000 bags, cancelled 500 flights and made losses of GBP £16 million

Multiple problems struck during the Terminal's first few days such as:

- Major IT problems - especially with the baggage handling system
- Inadequate staff training
- Inadequate car park size for staff (unable to park when their car parks became full)
- Staff security searches were delayed
- Around 10% of lifts (elevators) not working
- Construction work on parts of the building not finished

By far the most significant problem was the impact of the malfunctioning IT baggage system

BA puts the failure to spot the IT issues down to inadequate system testing, caused by delays in construction work on the Terminal. (Construction work was scheduled to finish on 17 September 2007 - however, delays meant BA IT staff could not start testing until 31 October). Several trials had to be cancelled, and BA had to reduce the scope of system trials because testing staff were unable to access the entire Terminal 5 site

"Clearly our reputation has been damaged, but I am satisfied that we understand around 95% of the issues that led to our problems," said BA's Chief Executive at the time. "We are now working very hard to demonstrate that Terminal 5 is and can be a fantastic success

Note - LHR's Terminal 5 is actually owned and operated by the British Airports Authority (BAA). The Terminal is (was at the time) used almost exclusively by British Airways as their global hub

*Business Continuity **'lessons learned'***

1. **Testing**

   By following typical BC standards, best practices etc. - critical IT, telecommunications and mechanical systems would have been adequately tested prior to 'live use'

2. **Staff Competency** and **Training**

   Typical BC standards, best practice etc. - require that staff be competent for role and receive an appropriate level of training and exercising to achieve same

3. **Facilities** and **Resources**

   Pre-planned to be adequate for purpose e.g. staff numbers; car parking facilities etc.

4. **Exercising** (Rehearsal)

   Fundamental to the concept of Business Continuity is the need for an organisation to exercise (rehearse) for the various critical contingencies identified as major threats to its continuity of normal operations

   In the case of the Terminal 5 situation described above, it is likely that modular exercises of identified and individual critical matters - followed by at least one full simulation of the Terminal opening, would have obviated many of the problems experienced 'on the day'

   Note - it would have been necessary to hold the full simulation at an appropriate time interval prior to 27 March 2008 in order to provide a sufficient period for identified problems to be rectified. Ideally, a further full simulation should then have been run. Where problems with identified critical services could not be rectified in the appropriate period the opening of the Terminal could have been delayed - probably a better alternative to what actually happened

5. **Stakeholder Communications**

   BA's (& BAA's) communications with its customers, the media and other stakeholders / interested parties is generally acknowledged as being woefully inadequate

   Typical BC planning stresses the importance of adequately preparing for all forms of adequate stakeholder / other interested party communications at time of crisis - including appropriate 'communications' training and exercising

6. Other

There are several other BC considerations (not documented here) which - if implemented, would have further served to prevent or ameliorate what happened to BA and BAA as described above

7. Conclusion

Following and implementing typical BC standards, best practice etc. - prior to the opening of Terminal 5 - would have undoubtedly obviated most (if not all) of the problems actually experienced

https://www.computerweekly.com/Articles/2008/05/14/230680/british-airways-reveals-what-went-wrong-with-terminal.htm

Deliberately Blank

Case Study **4** (based on real events in the UK in 2009/10)

BA - Cabin Crew Industrial Action - UK - Late 2009 and throughout the first half of 2010

A brief overview

British Airways cabin crew voted to take (official) massive industrial action in the period immediately before, during and just after the Christmas and New Year holiday period 2009 / 2010 - threatening severe disruption to tens of thousands of customers over this peak holiday period. The reason for the strike was related to actions which British Airways proposed to take in order to reduce the effects of a severe (recession induced) financial crisis

British Airways' initial 'business continuity plan' in this case was to take the cabin crew union to a legal court in an attempt to prevent the proposed strike. The airline won that particular case on a legal technicality and the strike could not go ahead at that time - thus buying the airline a little more 'preparation time' and also saving the Christmas holiday plans of hundreds of thousands of people

By mid-March 2010 the cabin crew union did actually strike - as the previous legal ruling preventing this had now been successfully overcome. By this time British Airways (BA) had trained some 1000 'other' staff (including some pilots) as temporary cabin crew - and had also made arrangements to operate around 25 wet leased aircraft on BA services. The result was that around 60 to 65% of BA flights operated as normal throughout this specific strike

Further and longer strikes occurred during May / June but the airline was still able to operate some 60-70% of its services due to the measures already documented above

By July the dispute had almost been settled except for the main union demand that some staff travel concessions removed by BA management concerning certain striking staff should be reinstated. With BA management estimating that they could run 80% + of LHR flights during any further industrial action and more and more 'strikers' returning to work - the prospect of further industrial action was fading

*Business Continuity **'lessons learned'***

Where an organisation operates under the threat of relatively frequent and serious industrial action, mitigating BC strategy and tactical treatments should be pre-planned, documented, approved and implemented. However, great care should be taken to ensure that the chosen BC treatments themselves are not the cause of industrial action

Some examples follow:

1. Pre-arrange for appropriate Legal and Regulatory expertise to be provided at very short notice

2. Pre-arrange for appropriate *'volunteer '* staff competencies to be attained

   Train and exercise appropriate volunteer staff to take over the roles & responsibilities of potential strikers - to the level where a pre-agreed level of Business Continuity operations (MBCO) could be maintained in a very short timescale (RTO) - should such industrial action ever occur

3. Pre-arrange for appropriate short notice arrangements to be made to lease, charter or otherwise 'buy-in' aircraft and crew from external suppliers - to the level where a pre-agreed level of Business Continuity operations could be maintained if industrial action eventuates

   Adequate service level agreements should be put in place in order to support the above

4. Stakeholder Communications

   BA's communications with its customers, the media and other stakeholders / interested parties is generally acknowledged to have been good throughout this dispute. In particular significant and advantageous use of social communications / media (Twitter; Facebook etc.) was made by the airline

   Conversely, the union representatives were sometimes generally perceived as inflexible and confrontational - with deliberate plans to cause the most disruption to BA (and thus also to customers) at peak travel periods

5. Other

   There are several other BC considerations (not documented here) which BA implemented during the dispute, which served further to ameliorate the adverse effects of the industrial action taken

6. Conclusion

   Following and implementing appropriate BC strategy / tactical treatments during this dispute enabled BA to maintain a reduced but nonetheless significant level of operations

Whilst the financial costs must be considered in the shorter term (the strikes had cost BA around GBP £150 million as at July 2010) - good stakeholder / other interested party communications and customer service combined with the maintenance of operations to a significant percentage of normal operations level - can only have enhanced BA's image and reputation for the longer term, a vital factor in the viability and survivability of any organisation

https://www.guardian.co.uk/business/2010/jun/07/british-airways-20th-day-strike

https://www.bbc.co.uk/news/business-13373638

Deliberately Blank

Case Study **5** (based on real events in much of N. Europe in April & May of 2010)

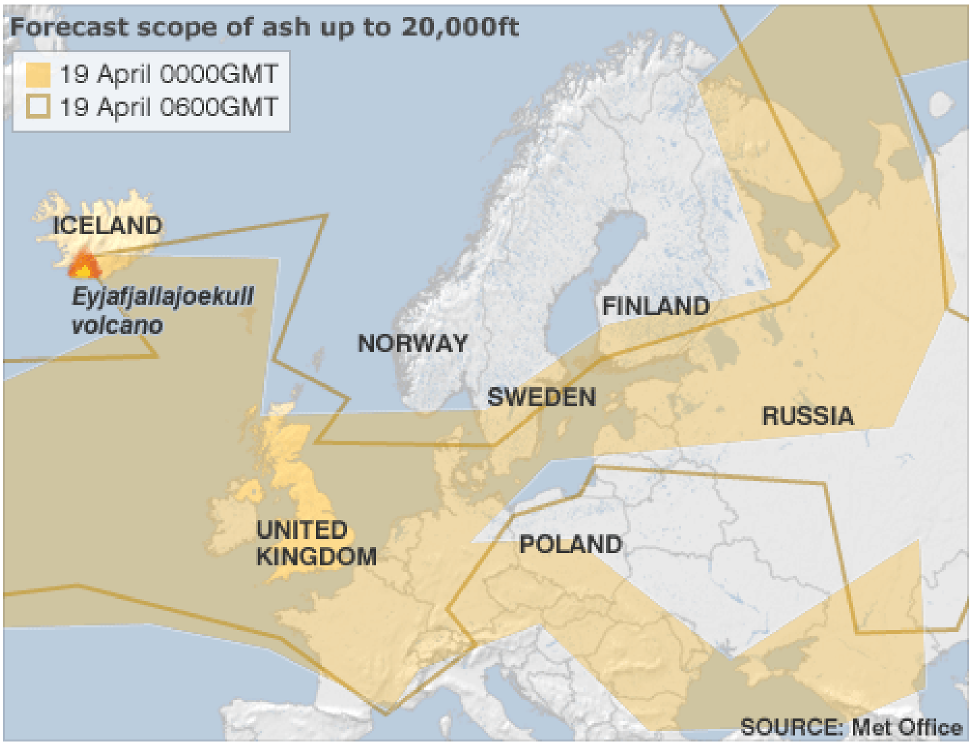
DISRUPTION to 'ABCX AIRWAYS' OPERATIONS (Due volcanic ash causing complete and prolonged closure of airspace in large parts of the Northern Europe and North Atlantic regions - during April and May 2010)

A brief overview

Note: For the purposes of this case study assume that *'ABCX Airways'* is a major European ***charter*** airline (inclusive tour / tour operator [passenger] airline) operating from numerous airports across the UK - mainly to short haul destinations (e.g. Spain, Portugal, Canaries, Madeira etc.) with some mid-haul destinations (e.g. Egypt) and a few long haul destinations (mainly in the Caribbean & S. Asia regions)

The airline is part of a parent company 'tour operator' which uses *ABCX Airways* to transport the vast majority of its customers - mostly on inclusive tour type holiday packages. However, the airline also offers 'airfare only' (seat only) flights

Where the terms 'disruption plan' or 'disruption contingency plan' are used in this case study - they are generally synonymous with the term 'business continuity plan and / or business recovery plan'



Source - UK Meteorological Office

Introduction

On Thursday 15 Apr 10 UK it slowly became clear to UK charter operator *ABCX Airways* that it was about to face the biggest operational disruption in its history due *complete closure* of all UK and Irish national airspace - together with other large areas of airspace across Northern Europe

The reason was the eruption the previous day of the EYJAFJALLAJOEKULL volcano in Iceland - along with prevailing middle to upper level winds at that time, which had blown the volcano's ash cloud across just about the whole of the UK and much of Northern Europe

EYJAFJALLAJOEKULL volcano - © Unknown

ABCX Airways was not alone in its trepidation that day as all other UK aircraft operators were also effectively 'grounded' in UK - including national carrier 'British Airways' and even the UK military (air force etc.). Furthermore, foreign aircraft operators with aircraft already on the ground in UK had effectively lost use of these aircraft - as did UK operators (including *ABCX Airways*) to a degree - with aircraft, crews and passengers stuck *outside* of the UK. The latter had not experienced anything like this disruption to its airspace since the Second World War

The same situation simultaneously prevailed across Scandinavia, Germany, some other North and Central European countries (extending as far east as Turkey) and parts of France

The knock-on effects immediately spread around the globe as some of the busiest airports in the world were suddenly closed to all flight operations. To make matters even worse there was no immediate prospect of the ash cloud shifting position significantly for around 7 days - based on the forecast wind movements in the region at the time

Although *ABCX Airways* was not to know it at this point - it would be recovering up to around 100,000 of its stranded customers from around the world from the time that flight operations resumed (effectively from 21 Apr 10) - with the vast majority being recovered by 26 April. Not all would be recovered by air - with some ten thousand returning via coach & ferry and / or chartered cruise ship

Until return transportation could be arranged, all stranded customers in general (including airfare / seat only customers where necessary) continued to be accommodated, fed and watered at the expense of the airline and its parent company - many in 'all inclusive' type accommodation

Why was the airspace closed?

Historically, volcanic ash and aeroplanes do not mix well. For jet aircraft especially there is a danger that flight through volcanic ash clouds can cause complete engine failure (all engines) plus other very undesirable effects. There are well documented cases of this occurring with almost tragic results - follow the below links for more information:

https://pubs.usgs.gov/fs/fs030-97/

https://en.wikipedia.org/wiki/British_Airways_Flight_9

Background

The first indication of possible problems to flight operations in UK and N. European airspace came on Wednesday 14 April - the day that the volcano erupted. By that evening *ABCX Airways* had invoked its ***disruption contingency plan*** to '**alert state YELLOW**' and formed a small crisis response team to deal with what it thought would be relatively ***moderate*** disruption

By 0300 local time the next morning (5 hours after declaring YELLOW alert) the extent of the pending disruption became clearer and the alert state increased to **ORANGE** - which equates to potential / actual disruption at ***serious*** level

Thereafter, flight operations through affected airspace gradually came to a complete halt during that day as the various aviation authorities involved closed down the affected airspace

https://news.bbc.co.uk/1/hi/8621407.stm

As the enormity of the disruption became clear to *ABCX Airways* '**RED Alert**' (potential / actual ***severe*** disruption) was declared and the full airline disruption plan invoked - involving 24H manning of the airline's crisis management centre (CMC) and 24H activation of a large disruption response (business continuity / recovery) trained and exercised team - sourced from both airline and parent tour operator personnel

The disruption response plan used to guide both the airline and tour operator response (to the volcanic ash crisis) was effectively an adaptation of a plan which had been prepared two years earlier for response to hurricane (natural disaster) related disruption - which had historically caused serious and occasionally severe disruption to the airline at its Caribbean destinations each hurricane season (May to November each year)

However, until much of the closed airspace re-opened, no disruption response plan could help *directly* - as no flying = no business = no business continuity. Therefore, the airline decided to use its existing disruption plan and supporting resources to ensure that business continuity and recovery measures could be implemented immediately the airspace restrictions were lifted

Note - Before looking at how the airline did this it might be useful to briefly outline the structure of the airline's existing disruption plan at the time of the volcanic eruption i.e.

- *Plan was documented and contained appropriate information; roles, responsibilities & accountabilities; procedures & checklists etc.*
- *Plan was relatively well practised due previous disruption responses to actual hurricanes; natural hazards in UK and overseas i.e. snow, ice, floods etc.*
- *Plan used 4 levels of alert related to actual / potential severity of disruption:*

○	***RED***	*= Severe Disruption*
○	*ORANGE*	*= Serious Disruption*
○	*YELLOW*	*= Medium (moderate) Disruption*
○	*GREEN*	*= Minor Disruption - as occurs to any airline regularly*

- *Initial disruption alert state generally decided and invoked by the duty manager of the airline's 24H Operations Control Centre*
- *YELLOW and GREEN disruptions generally handled as part of 'normal operations'*
- *For RED and ORANGE disruptions the **strategic** disruption response was generally removed from the 'normal operations' sphere and **formulated / managed** by a dedicated team known as the 'Disruption Response Team' (DRT)*
- *Much of the **tactical** RED / ORANGE disruption response was also **overseen** by the DRT*
- *The DRT convened regularly (typically four times per day during the volcanic ash disruption) during ORANGE alert - generally in the airline's CMC. Physical presence was preferred but attendance via telephone conference call was available if necessary*
- *A **core** element of the DRT convened permanently (24H) in the CMC during RED alert, on a 12 hour shift basis - otherwise the **full** DRT convened as for ORANGE alert*

- *DRT comprised (core DRT elements highlighted):*
    - *A person-in-charge (Director / SVP level) - known as the Crisis Director*
    - *A deputy Crisis Director (General Manager / VP level)*
    - *An expert facilitator from the airline's (full time) crisis / emergency / disruption response planning staff*
    - *An administrator (meeting minutes & general administration)*
    - *An airline operations control centre representative*
    - *An 'operational' tour operator (parent company) representative*
    - *A crisis communications representative - covering external (media), internal, website and social media type communications*
    - ** Disruption Support Unit (DSU) representatives*
    - *** A Humanitarian Assistance Team representative*
    - **** Other reps from parent group as required by disruption circumstances*

** DSUs comprise airline representation from the following individual business units:*

- ✓ *Airline / Aviation Planning*
- ✓ *Airports / Ground Operations (representing HQ and Outstations)*
- ✓ *Customer Services (including in-flight services / cabin crew)*
- ✓ *Engineering*
- ✓ *Facilities*
- ✓ *Finance*
- ✓ *Flight Operations (including flight crew)*
- ✓ *HR*
- ✓ *Insurance*
- ✓ *Legal / Regulatory Liaison*
- ✓ *Procurement*
- ✓ *Safety (Flight Safety & Ground Safety)*
- ✓ *Security*

DSUs operate in a similar way to that described for DSUs in Case Study 1

*** The ABCX Airways Humanitarian Assistance Team (also typically known as 'Family Assistance Team'; 'Care Team'; 'Special Assistance Team' etc. by some airlines / airports) is primarily formed to respond to a major aircraft accident type crisis - but is practically used on many occasions within the airline to also support all kinds of disruption from the humanitarian and welfare viewpoints*

**** Includes representatives from Commercial (Marketing, Retail, Call Centres etc.); Customer Service (Pre-flight, After Travel, Resorts etc.); Cruise Ships etc.*

***Top management** within the **parent** group also facilitated the means to escalate matters e.g. commercially or financially important decisions; matters concerning reputation, brand, image etc.*

The Airline's Response (UK Airspace Closed)

Note - assume that the 'airline response' also included that of the parent company tour operator

As the *ABCX Airways* peak summer season was still (luckily) a few weeks away from commencing (during this April phase of the volcanic ash disruption) the number of customers stranded overseas was low. It should be noted that we are speaking here in relative terms as the figure was still very large in absolute terms (tens of thousands) and continued to grow each progressive day as customers holidays finished but they could not get home (the numbers eventually peaked at around 100,000 persons)

Most stranded customers were concentrated in three regions i.e. Iberian Peninsula and the Balearics (Spain), the Canary Islands (mid-Atlantic Ocean) and Egypt

Whilst UK airspace remained closed the airline took immediate measures to bring home as many stranded customers as possible using all means available

In the meantime it implemented a major customer service, communications and information initiative - not only to those stranded overseas, but also to their families and friends in UK and, just as importantly, to those 'outbound' customers still waiting to go on their holidays from UK. This initiative also extended to all other appropriate stakeholders and other interested parties

Measures typically taken here included:

- Transporting (by coach) stranded customers from all over the Iberian Peninsula to a gathering point in NE Spain (near Barcelona) where they were generally given the opportunity to take a quick break in company provided hotels prior to being coached through France to the English Channel sea ports - for the short sea ferry journey to England, where onward coach travel was provided - in most cases to original airport of departure within UK

  Company (tour operator) resort staff from Spain escorted customers to the French channel ports where this role was transferred to members of the airline's UK based Special (Humanitarian) Assistance Team - who then remained with customers until they reached their original UK airport(s) of departure

- Using company cruise ship resources in the Mediterranean to ferry stranded passengers in the Spanish Balearic Islands to the gathering point near Barcelona - for onward coaching to and within UK - as described above

- Using stranded company aircraft and crews in Egypt and the Canary Islands to fly stranded passengers to the gathering point near Barcelona for coaching to UK (Mediterranean and Canary Islands airspace generally being unaffected by volcanic ash during April and thus open to normal flight operations)

- Chartering a brand new cruise ship (not company operated) to repatriate additional Iberian Peninsula customers direct to UK from a port in NW Spain. On arrival in UK the customers were then coached to their original airport(s) of departure. Company managers and Special (Humanitarian) Assistance Team representatives were already on the ship when it docked in Spain - and escorted customers throughout their journey to and within UK

- It is estimated that around 8 - 10,000 stranded customers were repatriated as described in the four bullet points above

- A major and high priority public communications campaign was launched to deal effectively and more than fairly with the tens of thousands of potential ***outbound*** customers also adversely affected by the disruption i.e. those waiting in UK to take their holiday packages, flights etc.

The Airline's Response (UK Airspace Re-opens)

At 2100 GMT on the evening of Tuesday 20 April the UK Government caved in to growing pressure (see article via link below) to re-open all UK airspace following a partial re-opening of airspace in Scotland and N England earlier that day - which had permitted *ABCX Airways* to launch a small number of repatriation flights into appropriate airports in the North of UK

Within minutes of this airspace re-opening the airline's crisis management centre took the decision to divert appropriate flights already in the air to northern UK destinations - to more commercially and operationally desirable destinations in the south - from where many customers had originally departed the UK

Since the first day of complete closure of UK airspace (Thursday 15 Apr 2010) the airline's planning and operations teams had produced and re-produced flight repatriation plans assuming that airspace would open the following day. Whilst this was extremely work intensive and non-productive on the days on which airspace remained closed - it also enabled the airline to implement a full repatriation flight programme at very short notice - starting during the early hours of 21 April and continuing until around 26 April, by which time some 85,000 stranded customers had ' come home'

The last stranded customers (mainly from long haul destinations) were all home by 28 April

The repatriation plan by air was the top priority for the airline - leading to the tough but logical decision ***not*** to operate outbound customer flights in general whilst positioning aircraft to the various airports overseas to pick up stranded customers. Again, a major effort was made to communicate and provide information and alternative options to delayed outbound customers and, in the main, this worked very well from reputational and customer service viewpoints

As the recovery operation continued and the backlogs reduced it became increasingly possible to resume flights for *outbound* customers. By around Wednesday 28 Apr 10 - some two weeks after the volcano first erupted, *ABCX Airways* was effectively back to normal operations status

Date - APR 2010	REPAT / Air	/ Sea	/ Coach	To Go	Total by Date	Cumulative Total
Tue 20	1500				1500	**1500**
Wed 21	10000		3500		13500	**15000**
Thu 22	15000		2500		17500	**32500**
Fri 23	15000	2500			17500	**50000**
Sat 24	13000				13000	**63000**
Sun 25	11000				11000	**74000**
Mon 26	9500				9500	**83500**
Tue 27				12000	12000	**95500**
Wed 28				3000	3000	**98500**
Totals	**75000**	**2500**	**6000**	**15000**	**98500**	

Recovery of *ABCX Airways* Customers stranded Overseas in April 2010 - situation as at 26 Apr 10. Figures are illustrative only but are a reasonable representation of the 'real' situation. Figures for 27 & 28 April were estimates

The Airline's Disruption Response Plan - Lessons Learned

It will be recalled that the airline *already* operated a robust, documented disruption plan with supporting infrastructure and resources (trained & exercised people, facilities, technology etc.) which had initially been targeted at response to hurricane induced disruption and similar - and which had been adapted to the volcanic ash situation - which is, after all, another form of natural disaster

In general this disruption plan worked extremely well in assisting in the various business continuity and recovery issues which eventually became evident and viable in a specific disruption event (threat / risk) which no one in the aviation industry had probably even remotely contemplated or specifically prepared for up to that point (something known in the crisis response / business continuity world as a 'Black Swan' event) i.e. the volcanic ash crisis

In light of this and other experience (see below) *ABCX Airways* committed to ***further*** develop its disruption response capabilities by producing a 'Significant Operational Disruption' contingency plan - with wider stakeholder / other interested party input than in the original disruption response plan, and also incorporating valuable feedback and 'lessons learned' from the volcanic ash disruption

Communicating with **Stakeholders** / other **Interested Parties**

It is generally recognised within the aviation industry and by the 'media' (in general) that *ABCX Airways* did an excellent job of communicating with all of its stakeholders / other interested parties throughout the crisis, especially in comparison to many other aircraft operators (airlines) similarly affected - and more especially with regard to other tour operator airlines

Stakeholders can range from customers and their families to legal and regulatory authorities - and just about anything else (as relevant) in between

The airline believed (correctly as it turned out) that this communication, in addition to its well documented record of effective, efficient and generous support to affected customers, would result in healthy return business and new bookings for the future

After-note

During mid-May 2010 *ABCX Airways* (amongst other airlines) was again confronted with serious to severe disruption caused by the returning volcanic ash cloud following fresh eruptions

It was now Summer holiday season for the airline when the volcanic ash cloud not only closed UK airspace again (partially and spasmodically) for a couple of days - but also closed the complete airspace associated with the Canary and Madeira Islands - where the airline (tour operator) again had tens of thousands of stranded customers

Whilst this disruption might be classified (and was) 'severe' - it only persisted for some two to three days until the airspace opened again and this, combined with the experience gained from the similar April disruption, meant a relatively quick business recovery to normal operations

Final Note - Thomson Airways is an ***actual*** charter (tour operator) airline which went through the above disruption for real in similar circumstances to that described for *ABCX Airways*. The newspaper article accessible via the link below makes interesting reading re some aspects of how Thomson Airways responded to the crisis. Note that to access this article today (written in September 2022) you will need to temporarily create and sign-in to a 'telegraph' account

https://www.telegraph.co.uk/travel/travelnews/7623988/Iceland-volcano-Inside-Thomsons-crisis-centre.html

And finally - a ‘tongue in cheek’ solution to volcanic ash problems on aviation!

© Unknown

Deliberately Blank

Case Study **6** (based on real events in May 2017)

Crash-landing for reputation of *world's favourite airline* - as **British Airways fails crisis management tests** (30 May 2017)

A brief overview

This case study combines 'how not to do it' from both Business Continuity and Crisis Communications viewpoints

It relates to how British Airways 'lost' most of its essential IT / ICT functionality in May 2017 - leading to absolute chaos around much of its world-wide flight operations network. It took until around 30 May to fully restore 'normal' operations

Details can be found by clicking / following the below link:

https://theconversation.com/ba-meltdown-crisis-researcher-caught-in-the-chaos-reports-on-a-massive-airline-failure-78487

Article (at end of above link) written: 30 May 2017

By: Denis Fischbacher-Smith (Denis.Fischbacher-Smith@glasgow.ac.uk)

Deliberately Blank

Case Study **7** (based on real events starting around December 2019)

Coronavirus (COVID-19) - Worldwide Pandemic

This case study updated in June ***2021***

Note

This case study 7 is fundamentally different from the preceding case studies

How and why is it different?

- **How**?

  The nature, scope, adverse impacts etc. of the ***COVID-19*** pandemic were typically (but not exclusively) ***unconducive*** to ***viable*** Business Continuity solutions by many of the various aviation related organisations (amongst many other types of organisation) directly and indirectly impacted

  This situation existed (in a very general context and to a greater or lesser degree) from about March of 2020 and was anticipated to continue (at time of writing this case study) up to ***at least*** the 1st / 2nd quarters of 2022

- **Why**?

  To inform the 'interested' reader that sometimes (rarely) a particular form / type / degree etc. of ***disruption*** might absolutely **NOT** have any ***viably*** effective, efficient, practical, timely, cost effective, non-hazardous etc. '***Risk Management*** / ***Business Continuity***' type solution(s) whatsoever

  The COVID-19 pandemic fitted this latter situation perfectly – most particularly for aviation related organisations and everything which relied upon them and / or upon which they relied e.g. tourism; essential resources (e.g. 'people' [staff / passengers etc. e.g. aviation fuel) etc.

The actual case study itself commences on the next page:

Case Study **7** (based on real events starting around December 2019 and updated as far as June 2021)

It has become 'fashionable' in *Risk Management* (and thus 'knocks on' to ***Business Continuity*** Management) to refer (generically) to ***very*** significant (adverse) impact disruption events as being a:

BLACK SWAN Event

A 'Black Swan' event / situation / occurrence (generally leading to massive 'disruption' [amongst many other adverse impact types]) typically ....

- Lies outside of rationale expectation as (typically [but not absolutely]) nothing like it will have happened before i.e. it is (almost) totally unpredictable
- Results in an extreme impact (good or bad [bad in the context ***used herein***])
- Despite its 'unexpectedness', there is a tendency for humans to lean towards producing an associated explanation(s) for its occurrence *after* the fact i.e. as if it had been explainable / predictable in the first place

Examples include 'World War 1' and the 'September 11th' terrorist attacks on the USA

OR (in contrast), a 'GREY SWAN' event is typically:

- Probable (to a greater or lesser degree)
- Predictable (to a greater or lesser degree)
- Capable of producing impacts which can easily cascade (for the good or bad [bad in the context used herein]) …………and
- Despite the 'predictability and probability', human nature tends to have an associated explanation(s) for such an occurrence - with typical emphasis on 'error(s) of judgment' / some other human related form of causation (where appropriate)

Examples might include Donald Trump becoming US President in 2016 and the UK leaving the European Union in 2021

OR (in further contrast), a 'WHITE SWAN' event is typically:

- Certain
- Has an impact(s) (for the good or bad [bad in the context used herein]) which is capable of being estimated
- Despite the 'certainty', human nature again tends to have an associated explanation(s) (sometimes irrational) for such an occurrence etc. (where appropriate)

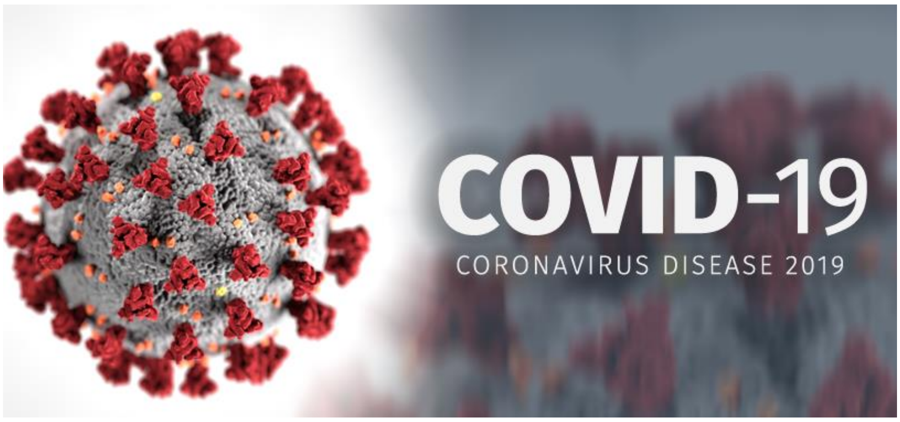
Examples include hurricanes (in season) in much of the Caribbean, West Coast Mexico, Gulf of Mexico and USA Eastern seaboard. Another is covered in an excellent (short) article (written in 'LGT' [Private Bank & Asset Management Group] on 20 May 2020 by 'guest' author Marc Lusterberger) - entitled:

The Corona (COVID-19) Pandemic: A White Swan - not a Black Swan?

You can read it by following the below link: (if link does not work try an appropriate internet search)

https://www.lgt.com/en/magnet/investment-strategies/the-corona-pandemic-a-white-swan-not-a-black-swan/#button1

This takes us on nicely to '**Case Study 7**' itself i.e. the **BC** implications for ***aviation*** (particularly airlines, airports, GHAs, airframe & engine manufacturers, aircraft maintenance organisations, aviation training organisations, associated holiday companies / tour operators etc.) of the COVID-19 pandemic:



In brief, the ‘knock-on effects’ of the COVID-19 pandemic were typically catastrophic / near catastrophic for many (if not most [possibly the vast majority]) of said (aviation related) organisations / businesses / similar

Such ‘effects’ also impacted adversely (to one degree or another - severely in many cases) e.g. on whole countries (states) - including those relying to significant degrees on the business, employment and other opportunities brought to them via ***aviation*** related resources e.g. tourism and other types of impacted commerce such as import / export via air-cargo of perishable foods; flowers; other impacted ‘goods’ delivered by air etc.

To expand a little further (but still at an overview / generic level only) it was factual and / or otherwise realistically ***anticipated at the time*** (around the April to September period of 2020) that:

- Many ***AIRLINES*** (including some of the ‘big names’) were unlikely to make a ‘viable’ comeback post-pandemic i.e. they would either cease trading altogether or need to trade in significantly different (e.g. smaller / operationally / commercially) ways than pre-pandemic (at least for some years). Some (a small selection) typical examples came under the following, actual ‘headlines’ at that time:
    - Easyjet plans to cut up to 4,500 staff
    - Virgin Atlantic to cut one third of staff in order to survive pandemic crisis
    - Air France / KLM boss starts discussions with unions re ‘big’ job cuts
    - Air Canada to lay-off 5,100 cabin crew
    - Air New Zealand to let go 3,500 staff (around 1/3 of its workers)
    - Norwegian Air temporarily lays off around 50% of its workforce (7,300 staff)
    - Scandinavian Airlines to temporarily lay off 10,000 employees (90% of staff)
    - Canadian operator Transat AT lets go 3,600 workers (70% of workforce)
    - British Airways puts 12,000 staff at risk of redundancy
    - Qatar Airways to cut more than 9,000 jobs
    - 3,400 management and admin jobs to be cut at United Airlines
    - Lufthansa to cut 22,000 jobs as it struggles to deal with coronavirus pandemic
    - Emirates cuts 1,000 pilot and 7,000 cabin-crew jobs - more cuts anticipated
    - TUI warns that up to 8,000 jobs would go as it strives to cut costs by 30%
- The knock-on from the above ***airline*** problems adversely impacted on many ***AIRPORTS***:
    - Some of the most important airline customers (including British Airways, Norwegian and Virgin Atlantic) at the UK’s ‘second’ airport (London Gatwick - LGW) anticipated that they might / would no longer use Gatwick going forward. Furthermore, the world’s biggest tour operator (TUI) had been a major airline customer (pre-pandemic) at LGW
    - Europe's biggest airport, London Heathrow, reported a £352 million ($USD 441 million) loss for the first quarter of 2020 (versus a profit of £102 million / $128 million for the same period in 2019). It said it ‘expected passenger numbers to be down by around 97% in April (due Covid-19) and that planned expansion, including a third runway, would be delayed by at least two years’

- Miami International Airport concession vendors collectively lay off 758 staff
- Over 1,200 workers were laid off from OTG (latter provides staff for restaurants & stores at New York's LaGuardia, JFK and Newark Airports)
- Workers have been laid off from Philadelphia, Orlando and Baltimore International Airports
- See below press article re Atlanta's 'Hartsfield-Jackson' International Airport:

ARTICLE

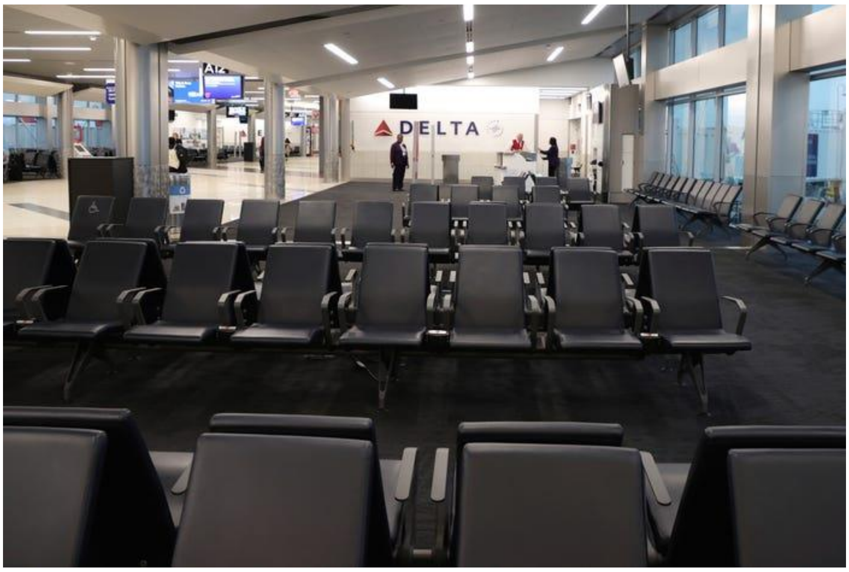
'Mostly empty' - Covid-19 has almost shut-down World's Busiest Airport

Hartsfield-Jackson international airport, Georgia's largest employer, has seen a huge loss of revenue and passengers

The Guardian:

Story by Khushbu Shah - Atlanta - ***13 April 2020*** (Last modified 1 July 2020)

Image Credit: Dawn Schnake / KCUR 89.3



A departure gate at an ‘almost empty’ Atlanta International Airport (mpi34/Media Punch /IPX/AP Images)

‘…………

Atlanta to Greensboro, North Carolina:	CANCELLED
Atlanta to Houston-Bush, Texas:	CANCELLED
Atlanta to Los Angeles, California:	CANCELLED
Atlanta to Milwaukee, Wisconsin:	CANCELLED

………. etc’

(Above) A ‘stylised’ sample of the departure board at Atlanta’s Hartsfield-Jackson international airport updates with cancellations due COVID-19 - whilst (below), nearly empty ‘Plane Train’ shuttles moved back and forth between seven largely empty terminals at that same airport

Though known as the world’s busiest airport and the State of Georgia’s largest employer, the COVID-19 pandemic and associated shutdowns have wiped out the passengers etc. at Atlanta’s Hartsfield-Jackson airport - and with them a revenue stream propping up the southern capital’s middle class

A city within a city, the giant airport’s success kept tens of thousands employed across the metro area, but as the airline industry takes brutal hits amid travel bans from Europe to the United States, its troubles are a huge blow for this airport and its city

“Revenue is probably down, off the top of my head, 50 to 60%,” the airport’s general manager, John Selden said, on a city council transport committee conference call at the end of March 2020

“We usually have 2,600 flights a day here, fully loaded - in other words, almost all seats taken. Right now, we’re down to 1,200 flights and they’re mostly empty.” The airport is ‘down 85% in passengers’ - he added

A staggering 63,000 people work at the airport when flights run at capacity

Among employees are thousands of airline workers, janitorial staff, restaurant staff and security - with a median salary of $71,500 - well above the city’s median income. Around 750,000 jobs are directly or indirectly tied to the airport across the USA’s south-east

END of ARTICLE

- The ‘interested’ reader might also wish to take a look at the info found in the below link:

https://www.businessinsider.com/coronavirus-haunting-photos-of-empty-airports-and-planes-2020-4?r=US&IR=T

- ***Ground Handling Operators***

  - The UK’s four main ground handling companies have warned that their operations at UK airports could grind to a halt in weeks, as the sector faces collapse

    Swissport, Dnata, Worldwide Flight Services & Menzies have written to the UK government to ask for financial support, as they face up to the impact of airline service cuts. They explain that currently more than 95% of flights are not operating, meaning that they (Swissport etc.) are not being paid

    Meanwhile, John Menzies (parent of Menzies) has announced it will cut job numbers by 17,500 (more than half its workforce [at 200 airports] worldwide)

OTHER

- ***Aircraft Engine and Airframe Manufacturers***

  - Boeing to cut more than 16,000 US jobs (with 4,000 more in the pipeline)
  - Aircraft engine manufacturer Rolls-Royce to cut 9,000 jobs
  - Bombardier to cut 2,500 aviation jobs as pandemic dents travel demand
  - Thousands of job cuts might be made across Airbus's global operations (furloughing more than 6,000 workers and 'bleeding cash' as airlines cancel or delay orders for new planes)

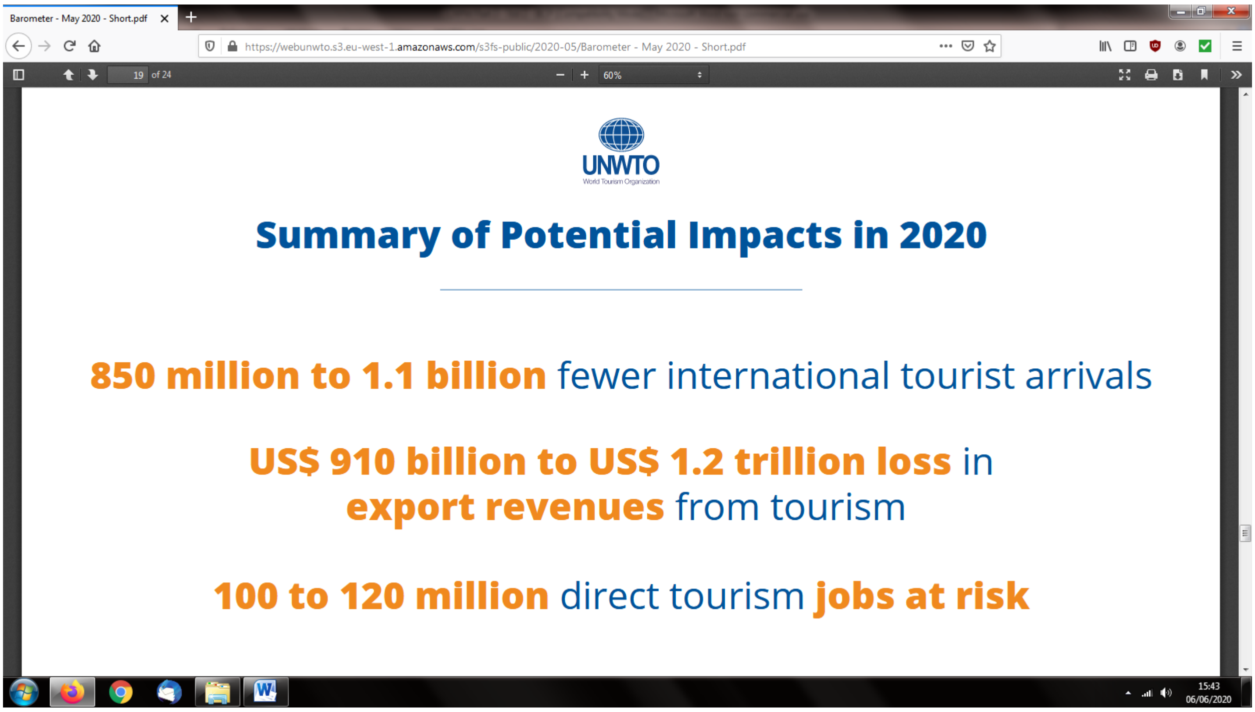
  For further related (historical) material see:

  https://en.wikipedia.org/wiki/Impact_of_the_COVID-19_pandemic_on_aviation

- ***Tourism*** (and thus the consequential knock-on effects e.g. for aviation) (This and next 8 pages)

  The boxed info a little further below gives a 'feel' for how tourism (with 'knock-on' effects to aviation of course) worldwide had been similarly (adversely) impacted by the pandemic. For more (historical) details see:

  https://en.wikipedia.org/wiki/Impact_of_the_COVID-19_pandemic_on_tourism


Barometer - May 2020 - Short.pdf
https://webunwto.s3.eu-west-1.amazonaws.com/s3fs-public/2020-05/Barometer - May 2020 - Short.pdf
19 of 24
60%
UNWTO
World Tourism Organization
15:43
06/06/2020

Summary of Potential Impacts in 2020

850 million to 1.1 billion fewer international tourist arrivals

US$ 910 billion to US$ 1.2 trillion loss in **export revenues** from tourism

100 to 120 million direct tourism **jobs at risk**

IMPACT ASSESSMENT OF THE COVID-19 OUTBREAK ON INTERNATIONAL TOURISM

United Nations World Trade Organisation (UNWTO) - ***Updated December 2020***

INTERNATIONAL TOURISM EXPECTED TO DECLINE 70% + IN 2020 (i.e. BACK TO 1990 LEVELS)

- The world is facing an ***unprecedented*** global health, social and economic emergency as a result of the COVID-19 pandemic
- Travel and tourism is among the ***most affected sectors*** with a massive fall of international demand amid global travel restrictions, including many borders fully closed, to contain the virus
- According to the latest issue of the UNWTO 'World Tourism Barometer', international tourist arrivals (overnight visitors) fell by ***72% in January-October 2020*** compared to the same period last year, curbed by slow virus containment, low traveller confidence and crippling travel restrictions
- The decline in the first ten months of the year represents ***900 million fewer international tourist arrivals*** compared to the same period in 2019 - and translates into an approximate loss of ***US$ 935 billion in export revenues*** from international tourism, ***more than 10 times the loss in 2009*** under the impact of the ***global economic crisis***
- Asia and the Pacific saw an 82% decrease in arrivals in January - October 2020. The Middle East recorded a 73% decline whilst Africa saw a 69% drop. International arrivals in both Europe and the Americas declined by 68%
- Data on international tourism expenditure continues to reflect very weak demand for outbound travel. However, some large markets such as the USA, Germany and France have shown recently some hesitant signs of recovery
- While demand for international travel remains subdued, domestic tourism continues to grow in several large markets such as China and Russia, where domestic air travel demand has mostly returned to pre-COVID levels
- Based on current trends, UNWTO expects ***international arrivals to decline by 70% to 75% for the whole of 2020***. This would mean that international tourism could have returned to levels of 30 years ago
- The estimated decline in internationals tourism in 2020 is equivalent to a loss of about 1 billion arrivals and US$ 1.1 trillion in international tourism receipts. This plunge could result in an estimated economic loss of over US$ 2 trillion in global GDP, more than 2% of the world's GDP in 2019
- Looking ahead, the announcement and the roll-out of a vaccine(s) are expected to gradually increase consumer confidence and contribute to ease travel restrictions
- UNWTO's extended scenarios for 2021 - 2024 point to a ***rebound in international tourism by the second half of 2021***. Nonetheless, a return to 2019 levels in terms of international arrivals could take ***2½ to 4 years***

INTERNATIONAL TOURIST ARRIVALS BY REGION

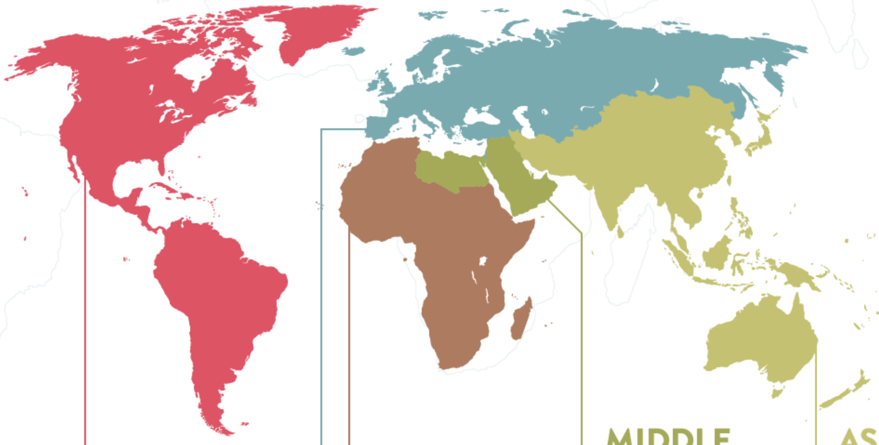
January-October 2020

2020 INTERNATIONAL TOURIST ARRIVALS

JANUARY–OCTOBER

WORLD

WORLD 2019: **1.5 BILLION (+4%)**
JANUARY–OCTOBER 2020: **-72%**



AMERICAS	EUROPE	AFRICA	MIDDLE EAST	ASIA & THE PACIFIC
2019 **219 MN (+1%)**	2019 **744 MN (+4%)**	2019 **70 MN (+2%)**	2019 **65 MN (+8%)**	2019 **361 MN (+4%)**
JAN–OCT 2020: **-68%**	JAN–OCT 2020: **-68%**	JAN–OCT 2020: **-69%**	JAN–OCT 2020: **-73%**	JAN–OCT 2020: **-82%**

UNWTO
World Tourism Organization

SOURCE: WORLD TOURISM ORGANIZATION (UNWTO), DECEMBER 2020

The UNWTO Confidence Index remains at record lows. Most UNWTO Panel Experts expect a ***rebound in international tourism by the third quarter of 2021*** BUT a ***return to pre-pandemic 2019 levels not before 2023***

The UNWTO Panel of Experts considers travel restrictions as the main barrier weighing on the recovery of international tourism, along with slow virus containment and low consumer confidence. According to this Panel, domestic demand would recover faster than international demand

UNWTO PANEL OF EXPERTS OCTOBER EDITION

Return to 2019 levels expected by 2023

UNWTO conducted a global survey among its UNWTO Panel of Tourism Experts on the impact of COVID-19 on tourism and the expected time of recovery. ***The survey was conducted during the first week of October 2020*** and the results are shown just below:

WHEN DO YOU EXPECT A REBOUND IN INTERNATIONAL TOURISM IN YOUR COUNTRY?

A majority of experts see a rebound in international tourism in 2021, in particular by the third quarter 2021, while around 20% expects it to occur sometime in 2022

WHAT ARE THE MAIN FACTORS WEIGHING ON THE RECOVERY OF INTERNATIONAL TOURISM?

Experts consider travel restrictions as the main barrier weighing on the recovery of international tourism, along with slow / low virus containment and low consumer confidence

WHEN DO YOU EXPECT INTERNATIONAL TOURISM TO RETURN TO PRE-PANDEMIC 2019 LEVELS IN YOUR COUNTRY?

Most experts do not see a return to pre-pandemic 2019 levels happening before 2023

IS DOMESTIC TOURISM DRIVING THE RECOVERY IN YOUR DESTINATION?

Domestic tourism is driving the recovery of several destinations but in most cases only partially, as it is not compensating for the drop in international demand. Respondents from Asia and the Pacific were the most positive regarding this matter

TRAVEL RESTRICTIONS

According to UNWTO's Report on COVID - 19 Related Travel Restrictions, as of 1 September 2020, a total of 115 destinations (53% of all destinations worldwide) have eased travel restrictions, an increase of 28 since 19 July. Of these, two have lifted all restrictions, while the remaining 113 continue to have certain restrictive measures in place. 93 destinations (43% of all destinations worldwide) are keeping their borders completely closed for international tourism. This is a decrease of 22 destinations compared to 19 July 2020

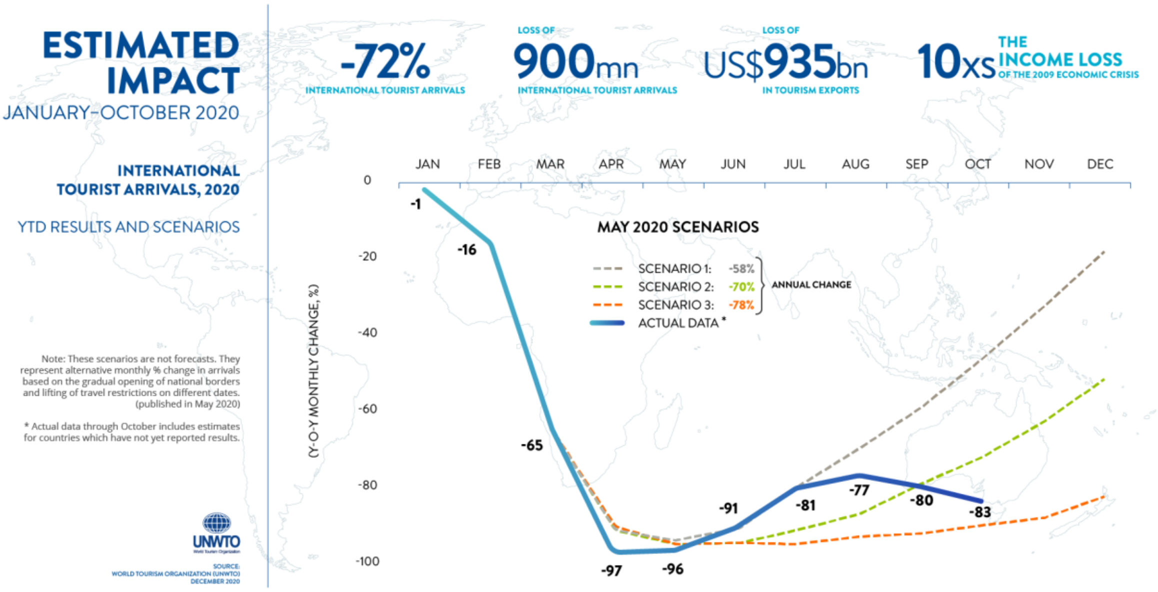
FORWARD-LOOKING SCENARIOS - 2020

UNWTO published three scenarios in May 2020, indicating declines of 58 - 78% in international tourist arrivals in 2020, based on the gradual opening of national borders and lifting of travel restrictions on different dates. (The scenarios are not forecasts and should not be interpreted as such)

International travel almost came to a complete halt in late March 2020 after the shutdown of most international borders, with arrivals plunging 97% in April, 96% in May and 91% in June. Results then 'edged up' slightly to 80% in July and 77% in August after some destinations gradually reopened their borders during the Northern Hemisphere summer season, particularly in Europe

However, as COVID-19 cases surged again in some parts of the World, many destinations re-introduced or stiffened travel restrictions, including compulsory quarantines and other measures, resulting in an 80% drop in arrivals in September and 83% in October

By early December 2020 most of these restrictions had not been lifted, though some destinations had shifted from a policy of complete closure to targeted restrictions. Still, other large destinations and source markets, as well such as China, remained completely closed to international travel. The latest data indicate that the year 2020 will end within overall decline of 70% to 75% in international tourist arrivals, putting results between Scenarios 2 and 3



Note: These scenarios are not forecasts. They represent alternative monthly % change in arrivals based on the gradual opening of national borders and lifting of travel restrictions on different dates. (published in May 2020)

* Actual data through October includes estimates for countries which have not yet reported results.

SOURCE: WORLD TOURISM ORGANIZATION (UNWTO) DECEMBER 2020

SCENARIOS FOR 2021 - 2024

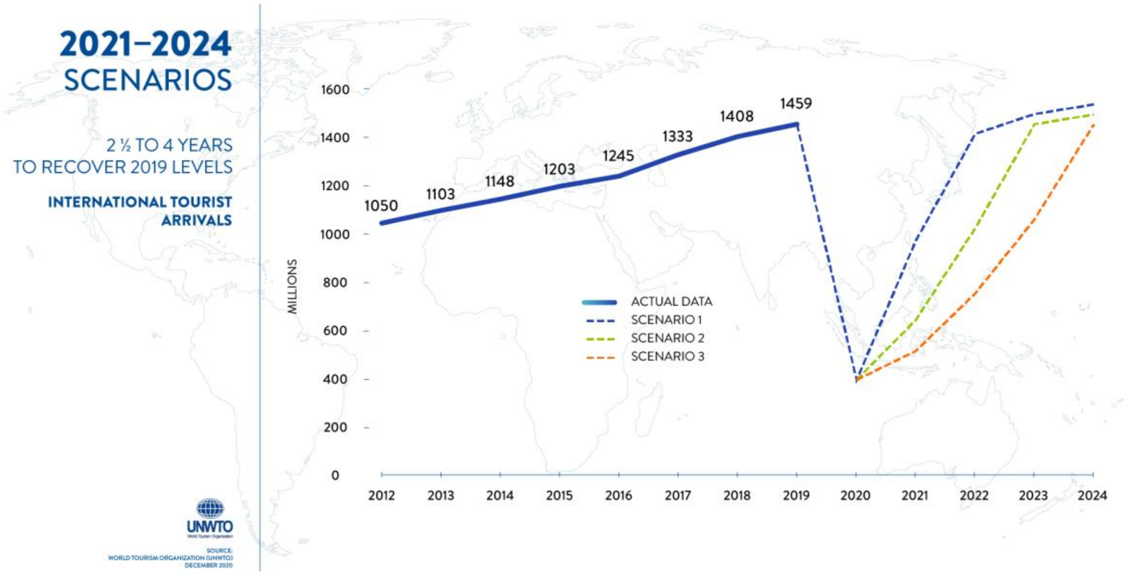
In the outlook beyond 2020, international arrivals are expected to rebound in 2021, based on the assumption of a gradual reversal of the pandemic, the roll out of COVID-19 vaccines, significant improvement in traveller confidence and major lifting of travel restrictions by the middle of that year. The expected rebound is also a consequence of the large pent-up demand after months of closed borders and travel bans. The extended scenarios presented here are in terms of yearly totals, not growth.

The rebound is expected to continue in 2022 as travel conditions normalise and the pandemic is contained globally. However, international tourism could still take 2½ to 4 years to return to 2019 levels. The recovery times for each scenario are summarized below:

Scenario 1: recovery in 2½ years (mid-2023)

Scenario 2: recovery in 3 years (end of 2023)

Scenario 3: recovery in 4 years (end of 2024)



KEY CONSIDERATIONS

- ***Pandemic***

  How long the pandemic will last and when will a vaccine(s) become readily available?

- ***Lifting of travel restrictions and lockdown measures***

  When will countries start easing restrictions and how will social distancing rules impact supply?

- ***Consumer & Business confidence***

  How long it will take consumers to reassume travel and how will travel behaviour change?

- ***Economic impact***

  How deep and how long will the global recession be and what will be consumers’ discretionary spending decisions?

- ***Governments Measures***

  How will government measures support tourism?

STRENGTHS • Proven resilience of tourism in past crises • Domestic tourism can be a buffer • Adaptation capacity: safety and hygiene protocols, trips closer to home, value for money, responsible consumer behaviour • Government support to the sector	**WEAKNESSES** • Segments potentially affected are also high spenders: international, long haul, business travel and events • Major disruption in airline industry with airline failures and concentration • Lack of references in previous downturns • Perception of travel as a risk • Low levels of demand when restarting tourism due to social distancing	**INTERNAL FACTORS**
OPPORTUNITIES • Re-think business model • Innovation and digitalization • Sustainability and sustainable-oriented segments (rural, nature, health) • De-escalation phases initiated by several countries toward the ‘new normal‘ • Progress in adaptation plans in destinations & companies	**THREATS** • Economic environment: world recession, rising unemployment and jobs at risk, closure of business mainly SMEs, disposable income, uncertainty weighing on consumer and business confidence • Uncertain length of pandemic (including resurgence) and vaccine unavailability • Extent of lockdowns and travel restrictions • Unknown form of the "new normal"	**EXTERNAL FACTORS**
POSITIVE	**NEGATIVE**	

Tightened Travel Restrictions Underline Current Challenges for Tourism

All Regions - **8 March 2021**

One in three of the world's destinations are now closed to international tourism. According to the latest data from the World Tourism Organization (UNWTO), the emergence of new variants of the COVID-19 virus has prompted many governments to reverse efforts to ease restrictions on travel, with total closures to tourists most prevalent in Asia, the Pacific and Europe

The UNWTO 'Travel Restrictions Report' provides a comprehensive overview of the regulations in place in ***217 destinations worldwide***. While previous editions had shown a movement towards easing or lifting restrictions on travel, the latest report shows that the ***persistent seriousness of the epidemiological situation has caused governments to adopt a more cautious approach***

As of the beginning of February 2021, ***32% of all destinations*** worldwide (69 in total) were completely closed for international tourism. Of these, just over half have been ***closed for at least 40 weeks***. A further ***34% of all such destinations were partially closed*** to international tourists

UNWTO Secretary-General Zurab Pololikashvili says: *"Travel restrictions have been widely used to contain the spread of the COVID-19 pandemic. Now, as we work to restart tourism, we must recognise that restrictions are just one part of the solution. Their use must be based on the latest data / analysis and consistently reviewed to allow for the safe and responsible restart of an industry upon which many millions of businesses and jobs depend"*

Regional Variations Clear

This edition of the UNWTO Travel Restrictions Report shows that ***regional differences with regards to travel restrictions*** remain. Of the 69 destinations where borders are completely closed to tourists, 30 are in Asia and the Pacific, 15 in Europe, 11 in Africa, 10 in the Americas and 3 are in the Middle East

At the same time, UNWTO research indicates a trend towards adopting a more ***nuanced, evidence and risk-based approach*** to implementing travel restrictions. For example, a growing numbers of destinations worldwide now require international tourists to present a negative ***PCR / Antigen etc. test upon arrival*** and also provide contact details for tracing purposes. Indeed, 32% of all worldwide destinations now have the presentation of such tests as their main requirement for international arrivals - often combined with quarantine - whilst a similar percentage have made testing a secondary or tertiary measure

Top Tourism Markets Remain Cautious

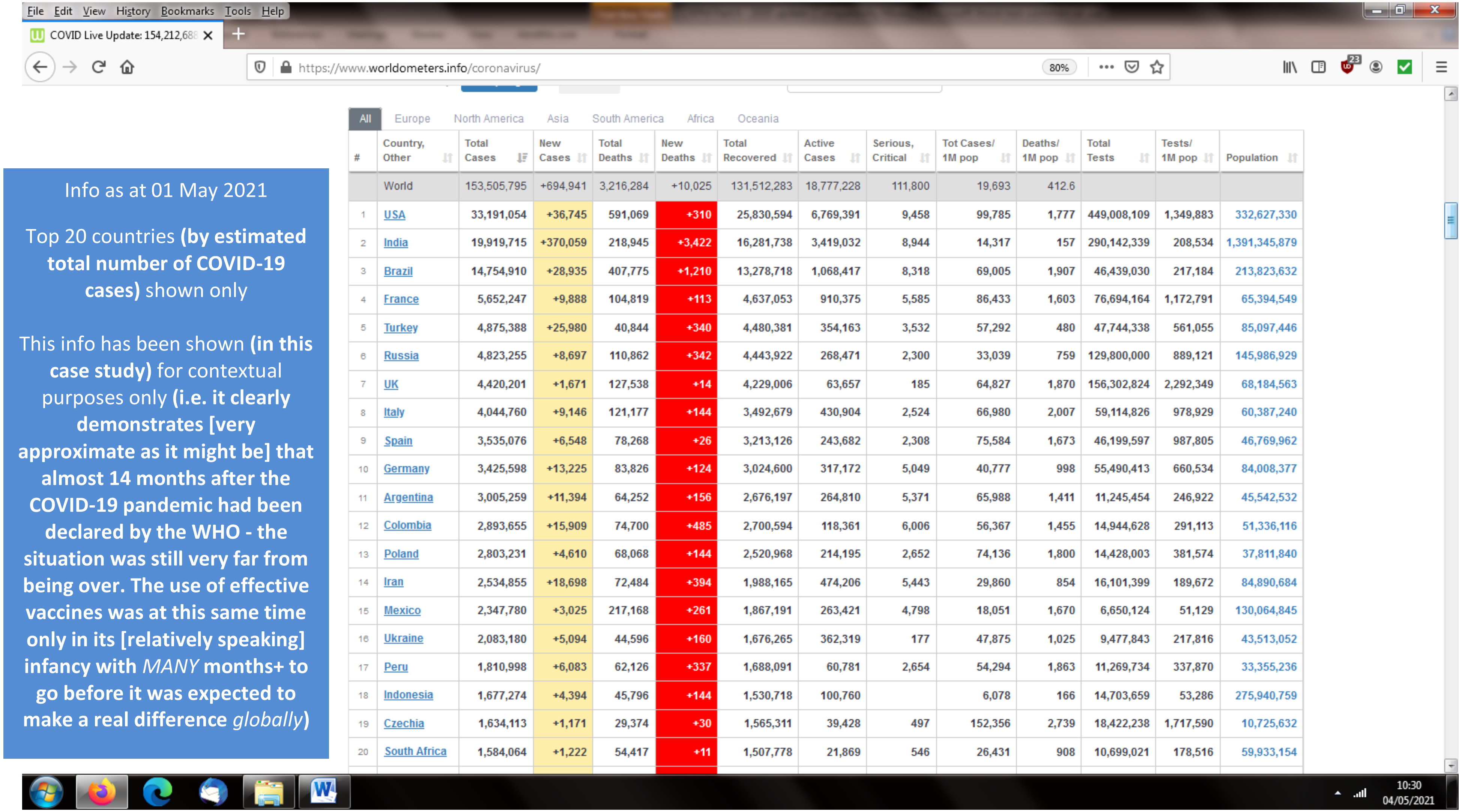
As UNWTO leads the restart of tourism, the 'Travel Restrictions Report' also notes how different governments are issuing advice to their own citizens. Analysis of the ***top ten tourism source markets currently advising against non-essential travel abroad*** found they generated 44% of all international arrivals in 2018. UNWTO notes that advice issued by governments will play a crucial role in the restart and recovery of tourism in the weeks and months ahead

Deliberately Blank

Info as at 01 May 2021

Top 20 countries **(by estimated total number of COVID-19 cases)** shown only

This info has been shown **(in this case study)** for contextual purposes only **(i.e. it clearly demonstrates [very approximate as it might be] that almost 14 months after the COVID-19 pandemic had been declared by the WHO - the situation was still very far from being over. The use of effective vaccines was at this same time only in its [relatively speaking] infancy with** ***MANY*** **months+ to go before it was expected to make a real difference** ***globally*****)**

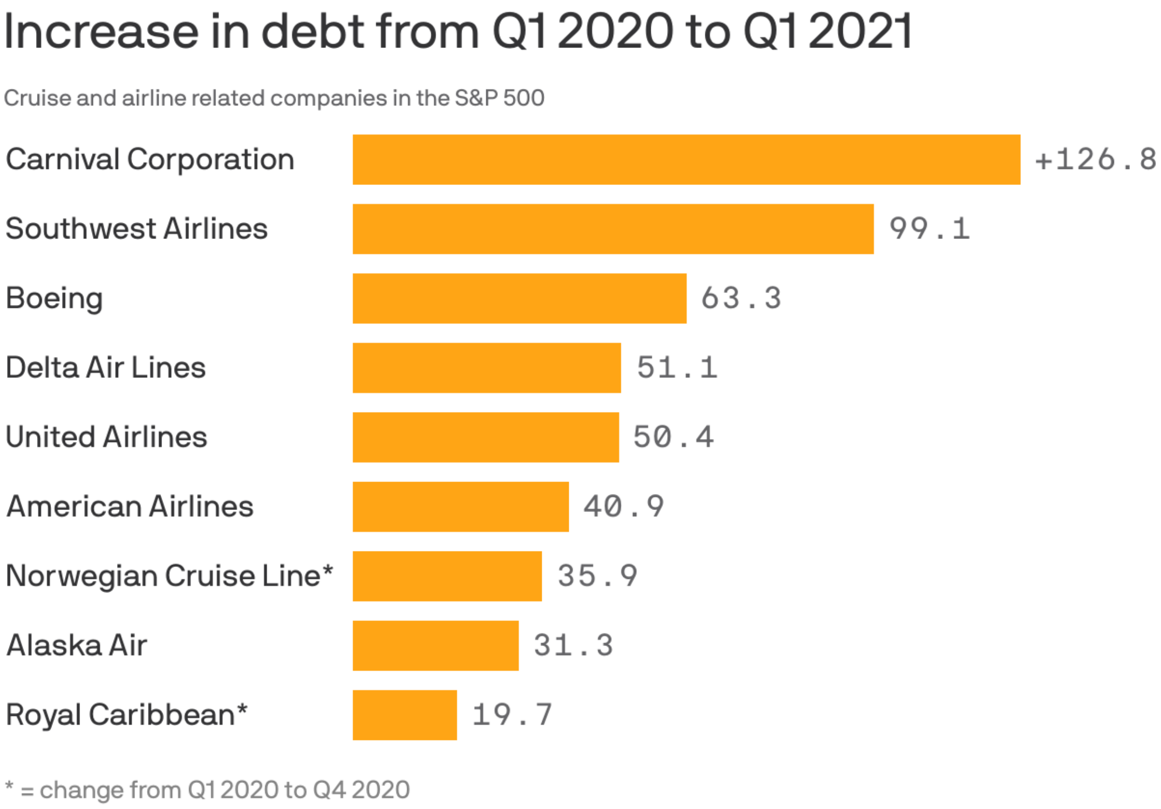

File Edit View History Bookmarks Tools Help
COVID Live Update: 154,212,68
https://www.worldometers.info/coronavirus/
80%
10:30
04/05/2021

All | Europe | North America | Asia | South America | Africa | Oceania

#	Country, Other	Total Cases	New Cases	Total Deaths	New Deaths	Total Recovered	Active Cases	Serious, Critical	Tot Cases/ 1M pop	Deaths/ 1M pop	Total Tests	Tests/ 1M pop	Population
	World	153,505,795	+694,941	3,216,284	+10,025	131,512,283	18,777,228	111,800	19,693	412.6			
1	USA	33,191,054	+36,745	591,069	+310	25,830,594	6,769,391	9,458	99,785	1,777	449,008,109	1,349,883	332,627,330
2	India	19,919,715	+370,059	218,945	+3,422	16,281,738	3,419,032	8,944	14,317	157	290,142,339	208,534	1,391,345,879
3	Brazil	14,754,910	+28,935	407,775	+1,210	13,278,718	1,068,417	8,318	69,005	1,907	46,439,030	217,184	213,823,632
4	France	5,652,247	+9,888	104,819	+113	4,637,053	910,375	5,585	86,433	1,603	76,694,164	1,172,791	65,394,549
5	Turkey	4,875,388	+25,980	40,844	+340	4,480,381	354,163	3,532	57,292	480	47,744,338	561,055	85,097,446
6	Russia	4,823,255	+8,697	110,862	+342	4,443,922	268,471	2,300	33,039	759	129,800,000	889,121	145,986,929
7	UK	4,420,201	+1,671	127,538	+14	4,229,006	63,657	185	64,827	1,870	156,302,824	2,292,349	68,184,563
8	Italy	4,044,760	+9,146	121,177	+144	3,492,679	430,904	2,524	66,980	2,007	59,114,826	978,929	60,387,240
9	Spain	3,535,076	+6,548	78,268	+26	3,213,126	243,682	2,308	75,584	1,673	46,199,597	987,805	46,769,962
10	Germany	3,425,598	+13,225	83,826	+124	3,024,600	317,172	5,049	40,777	998	55,490,413	660,534	84,008,377
11	Argentina	3,005,259	+11,394	64,252	+156	2,676,197	264,810	5,371	65,988	1,411	11,245,454	246,922	45,542,532
12	Colombia	2,893,655	+15,909	74,700	+485	2,700,594	118,361	6,006	56,367	1,455	14,944,628	291,113	51,336,116
13	Poland	2,803,231	+4,610	68,068	+144	2,520,968	214,195	2,652	74,136	1,800	14,428,003	381,574	37,811,840
14	Iran	2,534,855	+18,698	72,484	+394	1,988,165	474,206	5,443	29,860	854	16,101,399	189,672	84,890,684
15	Mexico	2,347,780	+3,025	217,168	+261	1,867,191	263,421	4,798	18,051	1,670	6,650,124	51,129	130,064,845
16	Ukraine	2,083,180	+5,094	44,596	+160	1,676,265	362,319	177	47,875	1,025	9,477,843	217,816	43,513,052
17	Peru	1,810,998	+6,083	62,126	+337	1,688,091	60,781	2,654	54,294	1,863	11,269,734	337,870	33,355,236
18	Indonesia	1,677,274	+4,394	45,796	+144	1,530,718	100,760		6,078	166	14,703,659	53,286	275,940,759
19	Czechia	1,634,113	+1,171	29,374	+30	1,565,311	39,428	497	152,356	2,739	18,422,238	1,717,590	10,725,632
20	South Africa	1,584,064	+1,222	54,417	+11	1,507,778	21,869	546	26,431	908	10,699,021	178,516	59,933,154

Deliberately Blank

And for those wanting an 'indication' of the 'cost' to the travel industry of the COVID-19 pandemic, in terms of increasing debt, see the below for a small but representative sample:



29 April 2021 - Economy & Business - Kate Marino Data: S&P Global Market Intelligence; Chart: Will Chase/Axios

The Pandemic might be Temporary - but the Debt is Permanent

Boeing reported another quarter (January - March 2021) of negative cash flow Wednesday, to the tune of $3.4 billion - its 6th consecutive, quarterly loss. The plane maker is one of many companies which borrowed from the capital markets heavily last year, even as the pandemic caused its revenue, and thus ability to pay interest, to shrink

Why it Matters: Piling on new debt helped businesses etc. to survive the immediate crisis, but borrowing their way through the turmoil now puts some at risk of becoming "zombie" companies i.e. can still operate but can't pay off their debts and / or invest in growth

The Big Picture: A slew of high yield companies took on billions more in debt during Covid-19 (to date), in some cases increasing their balances by more than half. Many of them (think cruise operators, airlines and the tourism industry in general) may not see earnings fully rebound any time soon

By the Numbers: Boeing sold $25 billion in bonds last May - one of the largest non-M&A bond deals ever, boosting its total debt balance to $64 billion from $39 billion

- The bond deal helped it avoid running out of cash as it struggled delayed aircraft sales and its grounded 737 MAX jet, the Wall Street Journal reported. (Regulators began *lifting the grounding* in November 2020, and Boeing aspires to generate cash flow in 2022)

Delta, United Airlines and American Airlines all got financial lifelines as each burned through millions per day

- Air travel has started pick up alongside widespread vaccinations, and though all three airlines reported net losses in their last quarters, they all returned to positive cash generation in March 2021
- Trade group 'International Air Transport Association - IATA' estimates that flight volumes won't return to pre-coronavirus levels until 2023 at the earliest

Carnival more than doubled its debt load, to $33 billion from $14 billion, as governments issued no-sail orders

- ***Norwegian***'s debt has increased by 36% to $12 billion, while ***Royal Caribbean***'s grew by 20%, to $20 billion
- Some countries have begun to loosen cruising restrictions and all three operators have announced plans for international cruises this year. However, the USA's ***Center for Disease Control*** (CDC) has not yet lifted the no-sail order for cruises in US ports and the companies all reported billions in net losses in their most recent quarters

Context: The USA's Federal Reserve's historic asset purchase programs underpinned investor willingness to buy the bonds despite the companies' minimal earnings

Yesterday, Fed Chairman Jerome Powell signalled that the central bank "isn't thinking about thinking about" tapering the bond buying program any time soon or raising interest rates from their rock bottom levels" wrote Axios' Dion Rabouin

The Bottom Line: Positive economic momentum will help pandemic-stricken companies return to normalised levels of profitability. But they still have to address the drastic increases in their debt loads spawned by unprecedented times, while keeping up with investments in their core businesses

SUMMARY

So, (re the COVID-19 pandemic and its impacts upon the ***aviation*** [and travel; tourism etc.] related industry word-wide) which of the 'Swans' might best fit the actual circumstances?

Pedantically speaking, COVID-19 was a **White Swan** event

Practically, however, (and nicely demonstrating the 'inadequacy' of such definitions and concepts [so why have them at all one might wonder?]) the ***COVID-19 pandemic exhibited certain elements of all 3 'Swans'***

FOOTNOTE

From: 'Continuity Central.com' (below message released in ***March 2020***)

'BCI Publishes its Annual Horizon Scan Report'

'…………… BCI (Business Continuity Institute) has released the 2020 version of its Horizon Scan Report

Sponsored by BSI (British Standards Institution - the national standards body of the United Kingdom), the report reflects the concerns of business continuity and resilience professionals when looking ahead to anticipated threats

Note *(written in* ***June 2021****)* **from author of this CRPM Part 3 / Vol 2 - i.e. the document you are reading right now**:

'……… Interestingly, whilst COVID-19 is front-of-mind for business continuity managers around the world right now, ***when the above Horizon Scan SURVEY itself was actually conducted*** *(****probably sometime in the second half or 2019****?) the threat category '****Non-occupational disease****' (of which '****pandemic****' [including COVID-19 when it* ***eventually*** *'appeared'] was a* ***major consideration****) was* ***only*** *ranked as* ***SECOND from LAST*** *in the list of* ***Future Threats*** *(see page 20 of that report for details)*

If the survey had been conducted some months later, this result would have been very different!!! ………..'

The interested reader might also find the article (at the end of the below link) useful:

https://www.continuitycentral.com/index.php/news/business-continuity-news/5346-was-covid-19-a-black-swan-and-why-this-is-an-important-question

Deliberately Blank

Case Study 8 (based on real events starting around March 2020)

Coronavirus (COVID-19) - Worldwide Pandemic

Remote Working / Working from Home (Updated to August *2021*)

Note

Like Case Study 7, this example is fundamentally different from the preceding case studies (1 to 6) contained herein

The consequences of the COVID-19 pandemic (started March 2020 and still devastating much of the world in June 2021) required very significant numbers of 'employees / staff etc.' to 'work from home' (WFH) over much of the world

Of course, WFH as a general concept has always been important from Business Continuity / Resilience viewpoints but, until the above pandemic, it had been significantly ignored in practice by many, ***as it had never before been activated to anything close to the degree that it was for COVID-19***

Whilst it might (hopefully) be many years before the world again faces an equivalent situation, the following article provides some useful inputs from 'Remote Working / WFH' viewpoints

The article itself was first seen by the author / owner of this guideline document (the one you are reading now) via an on-line blog placed (on 13 August 2021) by Charlie Maclean-Bristol of 'PlanB Consulting'

See last para of the article for details of the authors

Building Resilience and Security for Long-Term Remote Working

Image - "Working from home," by Victoria Heath - CC BY License

13 August 2021

'………..This week Steve Dance and Andrew Lawton discuss the 'risks we need to address' as ***working remotely*** becomes an option for organisations across the UK……….'

'Remote working / working from home' is now a regular and accepted arrangement for many organisations due the ***COVID-19 pandemic*** 'forcing' them to quickly adapt to same, in order to keep their businesses running. The 'experience' has accordingly 'forced' the subject of resilience / business continuity onto many boardroom agendas

Taking the UK financial sector as an example, operational resilience (Business Continuity etc.) is gradually becoming a regulatory requirement as e.g. the Bank of England, Prudential Regulation Authority and the Financial Conduct Authority press on with their initiatives on financial sector resilience. Given the number of financial institutions announcing their intention for remote working to be considered as part of 'business as usual', security and resilience for such arrangements will thus fall under the auspices of these new regulations

At a national level rumours are circulating that the UK government is considering a 'right to work from home' initiative

In all likelihood, we may never return to working full time 'in the office' and are more likely to adopt a hybrid arrangement with e.g. the corporate / business office used as a meeting and collaboration venue - whilst the 'remote / home' office is used for day-to-day work

However, for many organisations / businesses etc. - relying on average domestic (remote / home) ICT (Information Communications Technology) provision for associated security and resilience matters can (potentially) dilute significantly (and even compromise) the overall security position of the parent organisation (e.g. by better facilitating attacks from hackers; from accidental disclosure etc.)

Even where remote / home working is focused on 'routine' work, the latter might still be time critical, involve sensitive / confidential data etc. Similarly, 'physical security' (of data; systems; devices etc.) is also a significant consideration to address

The security and resilience (or 'lack of' as the case may be) of the 'remote / home office' can thus influence both domestic and corporate environments.

In adopting a regular work from remote / home arrangement, a considerable number of potential, consequential threats to security, resilience etc. can arise - e.g. (list is far from being exhaustive):

- Physical Compromise of Remote / Home Workplace

  Utility failure, property damage, illegal activities (e.g. burglary / housebreaking) can potentially limit an individual's access to ICT services e.g. power failures can last for hours and possibly longer, adversely impacting on e.g. operational deadlines; e.g. if all (hardware) ICT resources (including information stored therein) are stolen etc.

  Remote / home workers might also be exposed to 'single points of failure' in their home broadband / internet and power services if appropriate solutions are not considered and applied e.g. around 4.7 million people in the UK suffered a broadband outage lasting more than 3 hours during the past year, with an estimated cost to the economy of some £1.5bn

  Events such as the August 2019 power cut, which cut power to 1.1 million households, create headlines but every single day thousands of homes etc. are left without power (for one reason or another) in UK

- Absence of High Resilience Firewalls / Blacklisted Internet Users (IP Addresses) etc

  Most remote / home access solutions are outside of perimeter (e.g. parent organisation's head office etc.) ICT defences and may thus rely solely on security features of home / domestic devices and services alone

- Unprotected / Vulnerable Devices attached to Local (Home) Networks

  Home ICT networks typically support several, different devices, all / some of which might be unknown and unproven to the parent organisation's ICT security staff. As there is typically little that can be done in terms of preventing additional, unsecured devices from being attached to home networks - a significant ICT security risk potentially exists here

Whist there may be (but not always) solutions to the threats outlined above (and considerably more which have not been listed), they too have deployment issues that can be difficult to manage in the remote / home working scenario - for example:

Solution 'Silos'

Mitigating the threats may require several 'point' solutions for each threat. Is it practical or desirable to secure remote / home workers in this way - and, if so, can the mitigations be applied and maintained consistently?

End-user Ability to Apply / Maintain Security Solutions

If several solutions are required to mitigate threats, is it reasonable to expect end-users to deploy and manage same e.g. solutions such as micro-UPS systems and high grade security software? For example, in a scenario where domestic broadband is lost, relying on an end-user (who may be under pressure e.g. to meet a deadline etc.) to perform recovery of connectivity operations might be seen as unreasonable in the circumstances

To really work as required, remote / home working security needs to be pervasive, persistent and 'baked-in'

Management / Oversight and Support of Remote / Home Workers

An organisation's service / help desk etc. needs to have appropriate 'tools' at its disposal to effectively deploy, monitor and support ICT and related security solutions - in essence, they need a management console to ensure that remote / home workers are working in a secure environment

To overcome the security concerns and ongoing management challenges, remote / home working requires a holistic approach to reliably implement associated security and resilience solutions for the remote / home worker. Many organisations are now looking for associated remedies. 'Best of choice' integrated solutions might typically include (list is far from exhaustive):

- Integral UPS to ensure critical work is not interrupted by power outages, surges etc.
- Security features which enforce security of sensitive / need for protection data
- Automated failover to secure mobile data services (to preserve connectivity) in the event of domestic broadband failure
- Enterprise grade management capability of providing visibility and control of supporting remote / home workers via e.g. a single console
- etc.

This article was first published on Continuity Central and has been written by *Steve Dance* who is an independent consultant specialising in business continuity and operational resilience at RiskCentric, and *Andrew Lawton* who is CEO of ResKube

For some alternative outlooks on the same subject covered in this ‘Case Study 8’, the information at the end of the following links might help, as might independent search and study

https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home

https://www.ncsc.gov.uk/guidance/home-working

https://www.forbes.com/sites/hillennevins/2021/05/19/new-dangers-of-working-from-home-cybersecurity-risks/