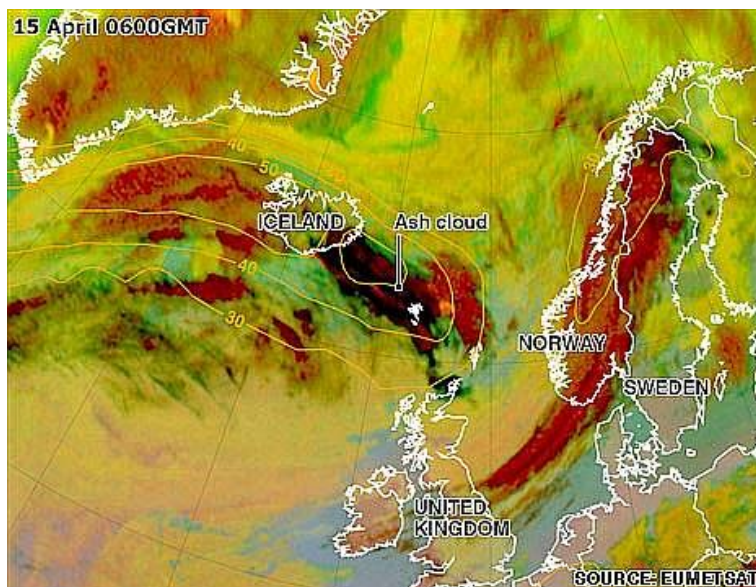




Guideline

CRISIS RESPONSE PLANNING MANUAL (CRPM) - Part 3

Business Continuity Management - in an Aviation Context



Above image shows volcanic ash plume from Icelandic volcano EYJAFJALLAJOEKULL - 15 Apr 2010 - at 0600 GMT (© EUMET SAT 2010)

The threat from the ash cloud to flight operations led to the total closure of much of Northern European airspace for almost a week - with combined losses of around \$2 billion+ US dollars to affected aircraft and airport operators, tour operators etc. This was the biggest closure of airspace since the Second World War. A similar ash cloud from the same volcano in mid-May 2010 also led to a suspension of flight operations in parts of Spain and all of the Canary and Madeira islands - with further disruption forecast again for as long as major eruptions of this volcano continue (Note - to date [2018] there have been no further [major] eruptions of this volcano)

This guideline (when used with other, appropriate guidance - [particularly international business continuity standard *ISO 22313:2012*]) - generally describes 'what needs to be accomplished' in order to be able to introduce a 'Business Continuity Management System' into an 'organisation'. Where appropriate, this guideline relates to an *aviation context* e.g. as might typically be useful to airlines, airports, ground handling operators etc.

www.aviationemergencyresponseplan.com (Parent Website to this Guideline Document)





EYJAFJALLAJOEKULL volcano April 2010 - © Unknown

20	AMSTERDAM	KL	1230	AF	8230	CANCELLED
25	BORDEAUX	AF	7622	AZ	3642	CANCELLED
25	MARSEILLE	AF	7662	DL	8362	CANCELLED
25	NICE	AF	7702	MK	9086	CANCELLED
25	TOULOUSE	AF	7782	DL	8582	CANCELLED
25	DUBLIN	EI	521		1	DELAYED
25	VIENNA	OS	412	AF	2638	CANCELLED
25	MALAGA	UX	1034	AF	2630	CANCELLED
30	NEW YORK-JFK	AF	012	DL	8654	CANCELLED
30	SEATTLE		306	DL	8628	CANCELLED
30	SAO PAULO		456			CANCELLED
30	HOUSTON		6	DL	8657	CANCELLED
30	CHICAGO		4	DL	8494	CANCELLED

© - unknown

IMPORTANT NOTE - This guideline document should be accompanied by an associated and appropriate course of training. To adequately ‘train’ for what is covered herein, it is envisaged that *at least* 5 full day’s training is required. For aviation related users - the training should be delivered by an appropriately competent, experienced person (with regard to Business Continuity matters) - who **also** has the appropriate, *aviation related background & experience*





Preamble - please read the following 'orientation' notes before proceeding further

Note 1 - The user / reader should clearly understand that in order to actually put the theory contained in this guideline document into real (actual) practice, from the 'ground up' (i.e. build, operate and maintain an actual business continuity management system * (BCMS) - for a large / complex airline, airport, ground handling operator etc.) is a major undertaking, typically requiring significant (up to one or more years) work. This assumes that just one or two persons (e.g. typically the 'Business Continuity (BC) Manager' + the alternate / back-up person [or equivalent(s)]) are assigned primary responsibility for the task

* For a *glossary* of terms used in this guideline - see page 24. For *acronyms* - see page 20

It is possible that smaller / simpler airlines, airports etc. *might* (repeat - 'might') be able to complete the task in a timescale which should be commensurately shorter e.g. say 6 to 12 months

Of course, it is not just 'work' that is required to establish a BCMS. For example - genuine, adequate, 'evidenced' and on-going commitment and support from top management will be essential - as will financing, procuring and allocating the considerable resources required, together with the achievement of appropriate levels of required 'competence and skills' (training & exercising) by designated persons. When all of this is in place, the BCMS will then require ever on-going maintenance, review and evaluation - including 'compliance' (audit) checks - throughout its entire life-cycle

Note 2 - As this guideline is studied, the user / reader will hopefully come to acknowledge (if not already convinced) that business continuity is now a must for most organisations - from the very smallest / simplest / local - to the most complex / largest / international

However, the concept of BC as a practical 'tool' has been around since mankind first evolved (see page 51) - so nothing new here? Well, there is actually something new i.e. since the industrial revolution and as part of the current 'technological (ICT) revolution', the risk that *certain* organisations will cease operations (for anything other than a *very* short period of time) - due to disruption of some type, is simply now *unacceptable* to society in general e.g.

- Hospitals
- Emergency Services (Police, Fire & Rescue, Ambulance etc.)
- Utilities (water; electricity; gas etc.)
- Telecommunications & Information Technology
- Distribution & Retail (food, fuel etc.)
- Transport Services
- Banking etc.

For similar political, legal, regulatory, commercial, financial, environmental, societal etc. reasons - BC is also now an essential requirement for the majority of 'organisations' in general (whether they realise it or not!)





For example, *a large and complex commercial organisation* (e.g. many airlines, airports and ground handlers) needs to keep 'trading / operating' (at least to a *pre*-defined level) - *despite any significant service / operational disruptions* (which could be caused by many different factors [*threats*] e.g. aircraft accident / incident; poor weather; ICT failure / disruption; utilities failure; industrial action by staff; use of facility denial [e.g. due fire, flood etc.]; security related incidents; public health incidents; volcanic ash; natural disaster; failure of supply chain; governance [legislation, regulation etc.])

The organisation tries to do this in order to avoid *unacceptable consequences* to those having an 'appropriate' interest i.e. stakeholders / other interested parties of all types, especially customers / clients and shareholders. One such 'unacceptable' consequence might ultimately mean *going out of business / cease trading or operating*

Conversely, now take a *single person trader* (say an auto / car repair business) - who might consider that BC is not appropriate for him / her. However, what if:

- The business premises are destroyed by fire
- The trader has an accident - keeping him / her off work for a relatively long period
- A critical part of the utilities supply fails e.g. electricity
- The external 'auto spare / replacement parts' delivery service ceases operation e.g. due bad weather; fuel shortage, sickness, closing down etc.
- The banking system used by the business has a major, longer-term IT failure
- Another auto repair business opens nearby - offering a 'better value (cheaper)' service with no corresponding degradation of quality etc.

Actually, the employment of BC measures (and the very closely related subject of 'risk management measures') *is* applicable to all of the above - and more e.g.

- The premises are destroyed by fire (Pre-cover this risk using insurance)
- The trader has an accident - keeping him / her off work for a relatively long period (Cover risk using insurance) *and / or* (employ contract labour for appropriate period)
- A critical part of the utilities supply fails i.e. electricity (maintain a suitable petrol / diesel generator [+ an adequate supply of fuel for same] on-site)
- The external 'spare / replacement parts' delivery service ceases operation e.g. due bad weather; due going out of business (maintain a reasonable 'on-premises' stock of the more common spare parts) *and / or* (have several different suppliers [not just the one])
- The banking system used by the business has a major IT failure lasting several weeks (use at least one other [different company] bank as part of normal business)
- Another repair business opens nearby - offering 'better value' services (build on your reputation and image e.g. using 'quality at a reasonable price' as the main influence for why current / potential customers should continue to use / consider using the business i.e. try to build and retain a loyal client base)





Note 3 - If an organisation (especially a 'larger and / or more complex' organisation) wishes to establish a BCMS for itself today (2018), it will probably need to refer (to a greater or lesser degree) to what is contained in the 'International Organisation for Standardisation's' BC * *guidelines* standard - known as **ISO 22313:2012**

* **Comment 1** - do **not** confuse use / context of the word '*guideline*' as used in the para immediately above - with the / this document (also known as a '*guideline*') - which you are reading now. **They are different!**

Comment 2 - **ISO 22313** is directly linked to its associated (but *separate*) BC *requirements* standard - **ISO 22301:2012**. The **former** provides **guidance** on how the **requirements** of the **latter** might be met

However, **ISO 22313** may also be used to guide any organisation to implement a BCMS, independent of **ISO 22301 requirements** - provided that formal certification to the **ISO 22301** standard is **not** required

Comment 3 - a whole BC 'vocabulary / terminology' has grown up around ISOs **22313** and **22301** (and their preceding 'national and industry' standards [now largely superseded] - upon which they have largely been based e.g. BS 25999). Accordingly, much of this vocabulary has been used in this guideline - and the user / reader should become very familiar with same. See Glossary starting on page **24**

Comment 4 - a brief overview of the **ISO 22313** and **ISO 22301 standards** can be found starting page **12**

Note 4 - The amount and variety of information contained in this guideline might appear daunting at first glance - and indeed, there is a lot to take in. However, do keep in mind that:

- a. The information provided needs to be sufficient for the larger and / or more complex organisations to be able to obtain and understand *all* of the *working basics* of what is required in order to implement a fit for purpose BCMS i.e. such organisations will typically require 100% (*and more - see note 4c below*) of what is included herein
- b. Some medium and most smaller and / or less complex organisations should be able to adapt / cut-down to a degree what has been referred to in item '4a.' above - commensurate with their own requirements - and provided that the BCMS essentials are covered (again, we are just referring here to the *working basics*)
- c. Any organisation will need all of the information contained herein (and more) if it is intended to meet (be *certificated* to) the *requirements* of BC Standard **ISO 22301**. The same applies (albeit to a lesser degree) if an organisation intends instead to make a *self-determination / self-declaration of alignment* with **ISO 22313**

Reminder: Any organisation can implement a BCMS - **without** the need for **ISO 22301** certification or even a self-determination / declaration of alignment with **ISO 22313**. However, such organisation will still generally require some form of guidance in the task – which is where **ISO 22313** might be able to help - at least to a limited degree





In order to achieve ISO 22301 certification, the minimum reference documentation required (i.e. over and above the guideline document you are now reading) typically includes:

- The BC '*requirements*' standard itself i.e. ISO 22301:2012
- The associated (supporting) '*guidelines*' standard for how the ISO 22301 '*requirements*' are to be met i.e. ISO 22313:2012
- ISO 22300:2012 - Vocabulary / terminology used in ISO 22301 & ISO 22313
- Possibly / probably ISO 31000:2009 (provides principles and generic guidelines of / on '*risk management*')
- Possibly / probably ISO 31010:2009 (guidance on '*risk assessment techniques*')
- Appropriate * further expansion / amplification of all of the above e.g. as contained in associated, specialist (mainly commercial) publications not already mentioned above - most of which will require purchase

* For example, performing a **Business Impact Analysis (BIA)** and associated **Risk Assessment (RA)** is generally acknowledged as the foundation of BCMS introduction into any organisation. Whilst this guideline (the document you are reading now) provides sufficient information to reasonably understand the *working basics* of BIA & RA in general - a certain amount of additional information [and pre-preparation] will almost certainly be required if they [BIA & RA] are to be accomplished and used successfully

Comment - generally speaking, all ISO standards require purchase

- d. Even if an organisation has no intention of achieving ISO 22301 certification - the use of ISO 22313 (in conjunction with this guideline document [the one you are now reading] + other, appropriate [commercially available] information) to assist in the planning, implementation, maintenance, review and evaluation of a BCMS into any but the smallest / simplest organisations, is nevertheless *very strongly recommended*

(However, do note the following quote from ISO 22313....."It is not the intention of this International Standard to provide general guidance on **all** aspects of business continuity")

Note 5 - To avoid confusion / for the sake of clarity - it must be clearly understood that this guideline document is *not* about simply putting together (producing) '*just a business continuity plan*'. Rather, it is meant to give the user / reader a good working knowledge of the **entire**, overarching process as to how a BCMS might relate to any organisation and, where so desired, then used further to *assist* in guiding the introduction of a BCMS into a particular organisation

As per above, one (*BUT only one of many*) BCMS implementation tasks requires the production of an associated **business continuity plan (BCP)** i.e. (and to re-iterate) the latter is *just one* of the many building blocks (another being e.g. 'personnel competency and experience' - achieved by training and exercising) required to establish a full, successful BCMS. Each and every such building block needs to be addressed *separately* i.e. *in its own right*





Note 6 - Prior to the 2012 introduction of (Business Continuity Standards) ISOs 22301 & 22313, there were a number of differing and unresolved viewpoints on the subject of 'business continuity' and its 'relationship' with the separate but closely related subject of 'risk management' - some of which (viewpoints) were undoubtedly driven by partisan / vested interests related to one or other of these subjects and the persons practising them!

The relationship is actually quite clear - i.e. business continuity is simply a **subordinate**, component element (known as a 'risk control' or 'risk treatment') of risk management i.e.

- Threats to an organisation are identified, analysed & assessed / evaluated - the evaluated results being expressed in terms of level of 'risk' to the organisation
- An 'informed' decision is made on what to do with (how to 'treat' or 'control') evaluated risks - e.g. ignore; avoid; transfer; manage / mitigate / reduce etc.
- One (but only one of several) method of managing / mitigating / reducing risk uses appropriate business continuity measures

The user / reader might ask '**why is this relationship important?**' The answer is that business continuity (BC) and risk management (RM) are so interdependently linked that neither can be ignored in their practical application. This is particularly so for BC and its (still historically unacknowledged by some) **subordination** to the parent / overarching RM processes

This relationship has always been evident within 'modern' BC - e.g. there is no point in completing a Business Impact Analysis (an essential BCMS 'building block') unless an associated 'Risk Assessment' is also undertaken - and the results merged, evaluated and managed

BUT - the BC 'experts' (ISO's Technical Committee [TC] 223) who put together ISO 22301 & ISO 22313 have now unfortunately (and possibly unnecessarily) gone beyond **simple risk assessment** (which is **relatively** easy to understand and implement) and significantly complicated matters by additionally including the need for.....(*quoting from ISO 22313*):

- Accountabilities and actions relating to 'risk strategy' and 'risk appetite'
- The need for establishment of a **formal** 'risk assessment' process
- The 'strongly implied' need to obtain, refer to (and understand) Risk Management standard 'ISO 31000:2009' (**Risk Management - Principles & Guidelines** - [24 pages / approximate price USD \$120]) and its supporting standard 'ISO 31010:2009' (**Guidance on Selection & Application of Risk Assessment Techniques** - [176 pages / approximate price \$320])

Accordingly (and the main reason for this Note 6), ISOs 22301 & 22313 have now, effectively, put an additional burden on those persons assigned BC responsibilities & accountabilities within an organisation - in that such persons will henceforth require (and / or require access to) a certain degree of risk management competence (knowledge & proficiency) - depending on the organisation's circumstances and resources. For example, where an organisation already has an effective & efficient RM Department / Business Unit - much if not all of the risk management aspects of BC may be assigned / delegated to that department / business unit





Indeed, many organisations combine the RM & BC functions (or, more realistically, BC is simply seen as a component part of an organisation's overarching RM roles & responsibilities)

However, the major problem here concerns organisations wishing to establish / update a BCMS - where no risk management expertise is internally available (i.e. beyond the ability to understand & apply *simple risk assessment* principles / implementation techniques) and where lack of appropriate resources (particularly money) does not readily permit engagement of appropriate *external RM* expertise (typically an RM consultant)

Should such organisations wish to be guided by *ISO 22313* (which is likely and actually recommended) - the job would be difficult enough if these 'new' BC requirements related to *risk* management were *not* there. But they are there and in their current form may be seen (perhaps not unreasonably) to have needlessly over-complicated an already (relatively) complicated process - whilst significantly increasing the already onerous awareness, competence and implementation burdens on those primarily involved

Note 7 - This guideline document (the one you are now reading) should *not* be used in isolation from *ISO 22313*

Cross-referencing to *ISO 22313* is widely used in this guideline document - as copyright matters do not generally permit direct reproduction of *ISO 22313* info herein. It is, therefore, desirable (*probably essential actually*) that ready access to *ISO 22313* is available to the user / reader (by whatever means - the simplest being to *buy* or *borrow* it) and that it is then referred to (via the cross references contained in *this* guideline [the document you are reading now] etc.) in order to reinforce and supplement (& possibly present slightly differing viewpoints in areas) what is written in *this* guideline (again - the document you are reading now)

Comment

Early-2018 price for *ISO 22313* (46 pages at around \$3.50 per page!) was around *USD \$160*; *ISO 22301* (24 pages at \$5 per page) costs around *\$120* and *ISO 22300* (12 pages at \$5 per page) comes in at *\$60*

The author / owner of this guideline document is of the opinion that 'societal security' type standards (including those above) should be *freely* accessible online i.e. at no cost to the consumer

For example and in contrast to the above, the equivalent *USA standard* covering Business Continuity (*NFPA 1600* [2018 version]) was *free* to view - see below extract from the associated US website:

'.....The 'National Fire Protection Association' (NFPA) strives to make its documents as accessible as possible, because we believe this is the best way to accomplish our mission

For more than 12 years, NFPA has offered free access to all of our codes and standards on our web site

To read a current edition of any NFPA code or standard, simply sign in at [nfpa.org/freeaccess](https://www.nfpa.org/freeaccess). Note that documents are read-only i.e. they cannot be downloaded or printed, because we rely on the revenues from people who want to own their own copies to fund the mission of NFPA. But for users who need to familiarize themselves with a code or check a requirement, this kind of access is invaluable.....'





As a matter of interest, NFPA 1600 is a purely national (USA) standard covering Disaster / Emergency Management and Business Continuity. However, if a US organisation trades internationally it would almost certainly be better to use ISO 22301 / 22313 (rather than NFPA 1600) if it wishes to demonstrate compliance (to stakeholders / other interested parties) with recognised BC standards. Many countries have already abandoned their national BC standards and adopted the associated ISO standards instead

Note 8A

- This original document (the '**work**') contains material protected under International and / or Federal and / or National Copyright Laws & Treaties. **Any unauthorised use of this material is prohibited**
- However, all & any entities & persons are licensed / authorised (by the copyright owner / original author of the work) to use the **work** under the terms of a 'creative commons licence'. (Follow the link below to see the **basic** terms of this licence in plain language (from there you can then also link to the 'legal' language version)):

[Attribution - Non-Commercial \(3.0\) Unported Licence - \(CC BY-NC 3.0\)](#)

Note - 'attribution' means placing the following (below) text in the header (or some other **prominent** position e.g. the page after the title page / front cover) of all and any derivative document(s) (known as 'adaptations') - which you make at any time - as based on this **work**:

'© AERPS / MASTERAVCON (A H Williams) - some rights reserved'

- For any **other** use of the **work** (e.g. use 'for commercial' / 'for profit or reward' purposes) - written permission is required. Such permission can be requested from:

info@aviation-erp.com

- The copyright owner / original author agrees that the term '**commercial**' (as used above) can be fairly interpreted as **not** applying to any use of this **work** as a template / guideline, where such use is made solely (only) for producing an emergency response plan or similar document (including a Business Continuity Plan and similar) - and where such use is solely (only) made by an entity (e.g. an airline, an airport) or a person(s) in the employ of such entity - for internal use by such entity alone
- If derived / adapted / changed versions (*adaptations*) of this **work** are made, then a statement to this effect must be placed in some appropriate, prominent position (e.g. the page after the title page / front cover) of all and any such derived / adapted / changed versions e.g.

'.....This is an adaptation of [insert title / name of the **work] by [AERPS / MASTERAVCON / A WILLIAMS (copyright owner and author)]**





- If adaptations of this **work** are made, it is recommended that all images in the original are replaced and / or omitted in the adaptation. This is in order to avoid any potential infringement of image copyright, which the original work copyright owner / author might reasonably be unaware of
- Entities and persons intending to distribute this **work** and / or its **adaptations** to other entities and persons, shall be responsible for ensuring that the terms, conditions etc. of this 'Note 8A' and the associated 'creative commons licence' referred to above, are passed on in turn. All entities and persons receiving such distributed versions shall then be bound by / subject to these same terms and conditions

Note 8B - Any person / entity having reasonable cause to believe that his / her / its copyright has been infringed in this document (**work**) - should please contact (email) the author soonest, in order that the issue can be mutually and satisfactorily resolved, without undue delay:

info@aviation-erp.com

Note 9 - An airline requires a suitably effective & efficient method of managing its emergency / crisis / incident / contingency response plans (including its Business Continuity Plan). A brief account of the method used in **this** series of guideline and guideline / template documents (one of which you are reading right now) will be found on page **16**. It is a well tried and proven method and it is recommended that airlines consider adopting same. If done, this will further strengthen the standardisation aspects of emergency / crisis / incident / contingency response plans amongst airlines and between airlines, airports and ground handlers

The above method can similarly be adopted and adapted for Ground Handling Operator use. However, the above method is **not** suitable for **airport** business continuity plans - which should generally be included as a component part (physical and / or virtual) of the **parent 'Airport Emergency Plan - AEP'** itself

Note 10 - Despite reasonable care being taken in the preparation of this series of guideline and guideline / template documents, they will inevitably contain errors, omissions & oversights, incorrect assumptions, links no longer valid / working etc. Readers / users identifying same and similar in this particular document (the one you are reading now) are requested to please notify (via email) the author / owner accordingly at - info@aviation-erp.com. Suggestions for improvement will also be gratefully received

The information contained in this document is provided on an 'as is' basis, without warranty of any kind. Whilst reasonable care has been taken in its preparation, the author / owner shall have no liability whatsoever to any person and / or entity - with respect to any loss, damage, injury or death caused (actual or allegedly) directly or indirectly and by whatever means - by use of such information

End of Preamble Section





Deliberately Blank





International Standards

ISO (Background Information)

ISO (International Organisation for Standardisation) is the world's largest developer of voluntary 'International Standards'. Founded in 1947, ISO has subsequently published more than 19,500 International Standards, covering almost all aspects of technology and business. Around 160 countries were members (in one form or another) of ISO as at 2018

A 'standard' is a document which provides *requirements, specifications, guidelines and characteristics* - which can be used consistently to ensure that *materials, products, processes and services* are fit for their intended purpose. Note that ISO's International Standards are not free i.e. they require purchase

Some of the first ISO standards issued were in the ISO 9000 (Quality Management) range - with perhaps the best known being 'ISO 9001 - Quality Management System Requirements'

International Standards are aimed at ensuring that products and services are safe, reliable and of good quality. For business, they are strategic tools which can reduce costs by minimizing waste and errors - and increasing productivity. They can also help organisations to access new markets, level the playing field for developing countries and facilitate free and fair global trade

Note - many countries produce their own *national* standards (similar in concept to ISO standards) on a vast range of subjects. Some take guidance from / are similar to ISO standards and some do / are not

In *some* subject matter areas the best of national standards have been combined to create an equivalent ISO 'international' standard - which then typically supersedes the associated national standards. An excellent example of this relates to *business continuity planning and operations* - see below

ISO - *Business Continuity* Standards

Up to 2012 a significant number of countries had produced their own national standards re 'business continuity'. In that year many (but not all) such national standards were superseded (with agreement of the countries concerned) by two, new international (ISO) standards:

- **ISO 22301:2012** - 'Societal Security - **Business Continuity Management Systems** (BCMS) - *Requirements*'

This standard specifies the *requirements* for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a *documented management system* to protect against, reduce the likelihood of occurrence, prepare for, respond to and recover from disruptive incidents i.e. a BCMS





The extent of application of these requirements depends on the various aspects of an organisation's operating environment and also its complexity

Organisations will *(if they so desire)* **be able to apply for formal ISO certification against the requirements of this standard** - and thus be able to demonstrate to legislators, regulators, customers (actual & prospective) and other interested parties that they are adhering to best Business Continuity Management (BCM) practice

Compliance with **ISO 22301** **OR** alignment with its *supporting standard* (**ISO 22313** - see further below) also enables the 'business continuity manager / equivalent person' to demonstrate to 'top management' / whoever - that a recognised, fit for purpose level of business continuity operation has been achieved by the organisation

ISO 22301 is necessarily formal in style (comprises short, concise **requirements** only) in order to facilitate **compliance auditing** and **formal certification**. Full compliance (no deviations) with its requirements is mandatory in order to achieve certification

However, a more extensive (and separate) standard (**ISO 22313:2012** - see next **main** bullet point further below) has been concurrently developed in order to provide greater detail (**guidance**) on each **ISO 22301 requirement**

Potential benefits of **ISO 22301:2012** certification include:

- Identification and management of current and future threats
- Taking a proactive approach to minimizing the impact of incidents on business
- Keeping critical functions up and running during times of crisis
- Minimising downtime during incidents and improving recovery time
- Demonstrating resilience to customers, potential customers, suppliers etc.

▪ **ISO 22313:2012** - 'Societal Security - Business Continuity Management Systems (BCMS) - **Guidance**'

This standard provides **guidance** for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a BCMS - thus better enabling organisations to prepare for, respond to & recover from disruptive incidents

It is not the intent of **ISO 22313** to imply uniformity in the structure of a BCMS - but rather for an organisation to design a BCMS which is appropriate to its own needs and which meets the requirements of associated 'interested parties / stakeholders' - including customers. Such needs are typically shaped by:

- Legal, regulatory, organisational and industry requirements
- The nature of an organisation's product(s) and / or service(s) etc.
- The processes associated with providing the product(s) and / or services etc.
- The organisation's operating environment
- The size and structure of the organisation





ISO 22313:2012 is generic i.e. applicable to all sizes and types of organisation, including large, medium and small entities operating in industrial, commercial, public and not-for-profit sectors - which wish to:

- Establish, implement, maintain and continually improve a BCMS
- Ensure conformance with the organisation's business continuity policy
- Make a self-determination / self-declaration of compliance with ISO 22313 (as required)
- Use ISO 22313 guidance to assist in achieving formal ISO 22301 certification (as required)

Where so desired, an alternative to *ISO 22301 certification* (the latter typically being a significant [work intensive / time consuming / resource related etc.] undertaking for many organisations) might be for an organisation to formally *align* its BCMS with *ISO 22313 instead*. If the latter is pursued, the work and other requirements etc. is / are still considerable, but the associated pressures related to 'certification' are removed

Note - *ISO 22301* & *ISO 22313* were developed in the main - based on the best of many of the preceding national standards referred to above. They are also the product of significant global co-operation & input

What is 'Societal Security'?

ISOs 22301 and 22313 were developed by ISO's Technical Committee (TC) 223 - the latter dealing with 'societal security' type issues i.e. developing standards for the protection of society from (and in response to) incidents, emergencies, disasters etc. - caused e.g. by intentional and unintentional human acts, natural hazards, technical failures..... and so on

TC 223's 'all-hazards' remit includes pro-active, adaptive and reactive strategies - which can be used before, during and after 'societal security' related events. The area of societal security is multi-disciplinary and typically (but not exclusively) requires active participation from both the public and private sectors

Some examples of TC 223's *other* projects have included:

ISO 22320:2011, Societal Security - Emergency Management - Incident Response Req'ts

* ISO 22315 - Societal Security - Mass Evacuation

* ISO 22322 - Societal Security - Emergency Management - Public Warning

* ISO 22324 - Societal Security - Emergency Management - Colour-coded Alert System

ISO 22398 - Societal Security - Guidelines for Exercises and Testing

* For example - as might be used in similar situations to the December 2004 Tsunami disaster in SE Asia; to Hurricane Katrina - August 2005 USA; to the Haiti earthquake - January 2010 etc.





Note from author/owner of this guideline document i.e. the document which you are reading now

The user / reader is reminded that the early 2018 purchase price for ISO 22313 was around USD \$160 - a lot of money for such a small document. For this price one would hope that ISO 22313 would comprehensively and clearly deliver its intent i.e. as a complete guideline to the implementation of ISO 22301's requirements. However (and in the informed opinion of the author /owner referred to above) it might be considered by some to be found wanting - for the following, general reasons:

- Despite ISO 22313's opening disclaimer of '*.....it is not the intention of this International Standard to provide general guidance on all aspects of business continuity.....*' common sense alone would indicate that at 46 pages it **cannot** come near to adequately providing the guidance needed to comprehensively complete what is a large and relatively complex project. For example, books have been written (in their own right) on the subjects of 'business impact analysis - BIA' and (separately) 'risk management (assessment) - RA', both of which are fundamental building blocks to the introduction of BCMS into organisations (BIA gets only a 1.5 page mention in ISO 22313 - and RA gets even less - at .75 of a page!!!!!!)
- Concerning *Risk Assessment*, ISO 22313 obliquely refers the user to another (*separate*) ISO standard - which would also require purchase i.e. ISO 31000:2009 ('*Risk Management - Principles & Guidelines*' - 24 pages / approx cost [early-2018] USD \$120). However, what ISO 22313 doesn't tell you is that in order to find your way around the 'risk assessment' bit of risk management, ISO 31000 has, in turn, its own related, supporting standard i.e. ISO / IEC 31010:2009 (*Guidance on Selection & Application of Risk Assessment Techniques* - 176 pages / approx price \$320)
- It is reasonable for an explanation of terminology used in ISOs 22301 & 22313 to be included within the documents themselves. This is not so. Yet again, a separate ISO document (ISO 22300 - \$60) needs to be purchased to get at this terminology
- ISO 22313's layout fails to follow the desired '**Plan / Do / Check / Act - PDCA**' cycle (*in contrast, the document which you are now reading does follow this cycle*). Instead, it (ISO 22313) follows a 'new' format for ISO management system standards (in general) introduced in 2012

The resulting document may be seen by some as being rather disjointed e.g. ISO 22313's Clause 6 (**Planning**) does not reflect 'planning' as envisaged in the PDCA cycle (for more on PDCA cycle see page 65 of this guideline document)

In summary, ISO 22313 is documented as being a guideline for the implementation of ISO 22301. In reality, many (most?) intended users will need to purchase additional ISO standards and other (non-ISO) commercial, specialist publications in order to successfully achieve such implementation. For some further context on this matter, see again 'preamble' Notes 4 (page 5) and 6 (page 7)





ABCX Airways (Preamble 'Note 9' on page 10 refers)

Crisis Response Planning Manual (CRPM)



The CRPM is the 'master' document which regulates and guides **all** forms of crisis / emergency / incident (contingency) response within 'ABCX Airways'

The CRPM is made up of 6 *separate* **Parts** - each part dealing with a specific type / aspect of an emergency / crisis / incident response - and containing associated accountabilities, procedures, checklists, information, explanations etc. The six 'Parts' of the CRPM are:





Deliberately Blank





Revision Information

This document comprises 303 pages - all dated 01 March 2018

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

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

** Based generally on ISO 22313

This document shall be reviewed and revised by its author / owner - on an 'as required' basis.

As a guide - the reviews should take place at no more than 6 monthly intervals. Should a review result in the need for a revision - then the revision will be prepared and incorporated, 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 be found at:

<http://www.aviationemergencyresponseplan.com/guideline-template/>

.....with title 'CRPM Part 3 - Aviation Related Business Continuity Planning'

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

Control of Documented Information

See page 119 before starting any tasks specified in this guidelines document (i.e. the one you are reading now)





Contents

Preamble		3
International Standards		12
The Crisis Response Planning Manual (CRPM)		16
Controlled Document Information		18
Acronyms / Abbreviations		20
Section 1	PRE-INTRODUCTION & GLOSSARY	22
Section 2	INTRODUCTION	50
Section 3	(Modern) ‘MANAGEMENT SYSTEMS’ & the PDCA CYCLE	65
Section 4/1	PLAN - For how BCMS should be introduced into an organisation	73
Section 4/2	PLAN - Resourcing the BCMS	104
Section 4 3	PLAN - Embedding awareness	113
Section 4/4	PLAN - Embedding competence	116
Section 4/5	PLAN - Communications	118
Section 4/6	PLAN - Documentation	119
Section 5/1	DO - DEVELOPING the BCMS - Op. planning & control	123
Section 5/2	DO - DEVELOPING the BCMS - Understanding the organisation	125
Note - Section 5/2 mainly relates to the ‘Business Impact Analysis’ and ‘Risk Assessment’ processes		
Section 5/3	DO - DEVELOPING the BCMS - Determining BC strategy	203
Section 5/4	DO - IMPLEMENTING the BCMS - the IRS + BC plans & procedures	229
Section 5/5	DO - IMPLEMENTING the BCMS - Exercising and Maintenance	249
Section 6 / 1	CHECK & ACT - BCMS performance evaluation	254
Section 6 / 2	CHECK & ACT - BCMS continual improvement	262
Section 7	CONCLUSION	264
Appendix A	CASE STUDIES	266
1 / SECOND GULF (IRAQ) WAR - 2003		267
2 / British Airways CATERING STRIKE (Industrial Action) - August 2005		274
3 / London Heathrow Airport - TERMINAL 5 CRISIS - March 2008		277
4 / British Airways CABIN CREW STRIKE - late 2009 to early 2010		281
5 / VOLCANIC ASH & AIRSPACE CLOSURES - April & May 2010		285
Appendix B - More on Risk Categories		297
Appendix C - Horizon Scanning		302





Acronyms / Abbreviations

BC	Business Continuity
BCPM	BC Programme Management
BCMS	BC Management System
BCP	Business Continuity Plan
BCT	Business Continuity Team
BIA	Business Impact Analysis
BRP	Business Recovery Plan
BRT	Business Recovery Team
CIQ	Customs, Immigration & Quarantine (Port Health) Services
DMC	Disruption Management Centre
DSU	Disruption Support Unit (see also IBU)
ERP	Emergency (Crisis / Incident) Response Plan
ERT	Emergency (Crisis / Incident) Response Team
IBU	Individual Business Unit (part of a larger entity) (see also DSU)
ICAO	International Civil Aviation Organisation
ICT	Information and Communications Technology
IRS	Incident Response Structure
ISO	International Organisation for Standardisation
MAO	Maximum Acceptable Outage (i.e. a period of time)
MBCO	Minimum Business Continuity Objective (i.e. an operationally related level of continuity - as related to provision of product, services etc.)
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 of Disruption (re a product, service, activity etc.)
RA	Risk Assessment
RCA	Resources Consolidation Analysis
RM	Risk Management
RPO (CDP)	Recovery Point Objective (Critical Data Point if relating to data/documentation)
RTO	Recovery Time Objective
SMS	Safety Management System
SPOF	Single Point of Failure





Deliberately Blank





Section 1 / PRE-INTRODUCTION

Purpose & Scope

The **purpose** of this guideline document is to:

- Provide a suitable reference source related to facilitating the acquisition of a **reasonable** level of **theoretical** knowledge - re the subject of business continuity in general - and **aviation** related business continuity in particular

Note - where a more in-depth knowledge is required, additional reference material should be consulted (see 'preamble' note 4c [page 5])

The **scope** of this guideline:

- Provides an appropriate depth and range of material, sufficient to permit a **foundation** (*reasonable*) level of understanding to be acquired - relating to the concept and **potential** practice of a '**generic**' Business Continuity Management System (BCMS) within a generic organisation **AND**
- Where appropriate - relates this generic BCMS to an aviation context
- Does **not** relate to the **specific task** (i.e. the **actual** work involved) of introducing a BCMS into an organisation (especially where this might be undertaken in conformance with a business continuity standard - e.g. **ISO 22301** and / or **ISO 22313**) - **BUT will nevertheless be found to be a very useful aid in such task** (see '**Objectives**' - next page)
- Generally excludes (for the sake of clarity, brevity and simplicity) **business continuity requirements and activities relating to the recovery of 'data'** - the latter being capable of existing in both soft and hard copy formats. In reality, however, this element of business continuity planning **must** be covered of course. The associated concepts / practices are relatively simple to understand and implement e.g.
 - Regular backups made of electronic data (the term 'regular' as defined by the organisation)
 - Electronic data backups to have an additional (adequate, secure & easily / rapidly accessible) 'off-site' storage capability
 - Hard copy documents to be stored in fire-proof repositories
 - Hard copy documentation of high importance to be copied and additionally stored in an adequate, secure & easily / rapidly accessible 'off-site' facility
 - etc.





Objectives

On successful completion of an appropriate course of training (as associated with the subject matter included in *this* guideline document) the typical user should be in a position to progress to the '*next phase*' - which is expected to involve the acquisition of Business Continuity (BC) related '*on-the job practical experience (and / or equivalent)*' - as will typically be required in order to eventually conduct effective and efficient **actual** (*real /practical*) BC activities, particularly with reference to aircraft, airport and other aviation related operations

Note 1: This guideline can be used as the foundation material for the associated training course

Note 2: The 'next phase' (as mentioned above) is **not** within the scope of this guideline

Context

- The major part of this guideline is written in the context of BC activities related to 'generic' organisations. This is deemed necessary in order for the user / reader to build up a solid BC foundation, with the aim of using it to progress (if and as required) to the application of BC in any practical context - *provided that suitable further training and / or experience and / or qualification requirements are met*
- Selected elements of this guideline provide an introduction to BC as it relates specifically to aviation. A medium to large sized operator / organisation (airline, airport, GHA etc.) has been assumed for this purpose unless stated otherwise.

However, the business continuity concept can be applied to just about any aviation entity, regardless of what the entity does - and of its complexity and / or size





Glossary (Know the' Jargon')

There is a significant amount of BC and * BC related terminology in use around the world and, as there has never been a truly *international* business continuity standard (until [arguably] the publication of ISO 22301 in May 2012 and ISO 22313 some months later), co-ordination of such terminology (to achieve international standardisation) between interested parties has never been *effectively* addressed / achieved

* Examples include 'Risk' Management, 'Emergency' / 'Crisis' / 'Incident' Response Management - etc.

That said, due credit must be given to certain organisations which *have* made some progress in the past - in at least documenting (but not being able to universally standardise) much of the terminology in use. Furthermore, the publication of ISOs 22301, 22313 and 22300 has helped in publishing a *limited* number of BC and BC related terms and definitions

However, (and notwithstanding that this guideline [the document you are now reading] is generally predicated on ISO 22313), the author / owner is currently (2018) of the opinion (subjectivity acknowledged) that BC terms & definitions might be better expressed (especially from a student's / trainee's perspective) using those in *current and actual common use right now* - albeit at the risk of losing an element of standardisation to a greater or lesser degree. This is what has been included in the following glossary and subsequently used in this guideline

Some inclusion of slightly *differing* explanations for the *same* term / definition has been made in the glossary where felt necessary - in order to better understand the meaning of the particular term / definition

It is anticipated that this guideline will transition exclusively to ISO 22300 / 22301 / 22313 terminologies - when same have reached an appropriate stage of maturity, 'completeness' and standardisation in actual widespread, international use - i.e. at some future time (but don't hold your breath for this to happen anytime soon!)

Note 1 - users / readers might find difficulty in fully understanding what is written in this guideline document unless the following glossary is both studied and understood

Note 2 - Audit procedure in detail is generally beyond the scope of this guideline document. Consequently, most audit-related definitions are not included in this glossary. However, see Sub-sections 6.1 and 6.2 of this guideline where limited information on the subject *has* been provided

Note 3 - this glossary is always capable of improvement (especially for those for whom 'English' is not a first language) - and all suggestions / proposals for such will be gratefully received by the author / owner of this guideline document (via email please) at:

info@aviation-erp.com





- **Activity**

Processes undertaken by an organisation (and / or on its behalf) - 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 aviation, 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 **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* etc. Processes are often inter-dependent with / on other processes. All require the 'support' provided by resources (especially people)

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 etc.)

An organisation's activities (+ everything they depend on) provide the major inputs for the two fundamental aspects of facilitating the management of business continuity - i.e. '**Business Impact Analysis**' and '**Risk Management / Assessment**' (sometimes otherwise known in common BC terminology as '**understanding the organisation**')

- **Alternate** (Recovery / Back-up / Fall-back) **Facility / Site**

An organisation's designated **secondary** facility / facilities, held in a pre-designated degree of readiness, in order to take over designated operations / services / activities etc. from the organisation's associated *primary* facility / facilities - when necessary e.g. an associated disruptive incident rendering the primary facility / facilities unavailable for a 'significant period' (latter term as defined by the organisation itself)

A '**cold**' alternate facility typically requires equipping, set-up, manning etc. 'on the day' (but in *extremis* may require building from the ground up). A '**hot**' alternate facility is generally fully equipped and set-up functionally - simply requiring manning (if not already manned) to make it fully operational. A '**warm**' alternate facility sits somewhere between the cold and hot sites described above





- **Backlog**

The effects on an organisation of an uncontrolled build-up of work / product etc. - which occurs as a consequence of an activity, process, resource etc. being temporarily unavailable and / or having a 'lower than normal' output

Note: a backlog may become so severe that it cannot be adequately cleared using normal resources - i.e. a "**Backlog Trap**" occurs

- **Business** (as used in a business continuity context)

The entire infrastructure, as associated with all aspects of delivering the final outputs (key products / services / operations) of a particular organisation - regardless of the latter's type, (e.g. Government / Public, Commercial, Not-for-Profit etc.) size, location etc.

- **Business Continuity** (BC)

An organisation's ability / capability to continue delivering its key products, services, operations, tasks etc. to an acceptable, pre-defined level - following a significant, disruptive incident (BC is a component of '**risk**' which is, in turn, a component of '**resilience**')

- **Business Continuity Context**

Identifying and defining the external & internal factors to be accounted for - when setting the scope and criteria related to producing a BC Policy statement - and also during on-going management of any BCMS programme

- **Business Continuity Management** (BCM)

The process of achieving, managing, maintaining and continually improving BC

- **Business Continuity Management System** (BCMS)

That part of an organisation's overall '**modern** management system' - which is applied specifically to 'business continuity management'

As with all modern management systems, a typical BCMS should include:

- A BCM **policy**
- **Management processes required to support** the BCM policy
- **Competent** (aware, trained, and exercised) **people** with pre-defined, documented & measurable BCM **roles, responsibilities and accountabilities**
- **Associated documentation** e.g. plans, information, instruction, guidance, etc. (also used to provide evidence as part of any audit / compliance process)





- An appropriate BCM *infrastructure*
- *Specific processes & procedures* required to support BCM
- *Other required BCM resources* - including budget, time, facilities etc.

- **Business Continuity Plan (BCP)**

Documented procedures designed to guide organisations in how to respond, resume, restore & recover to a pre-defined level of operation / service / output - following a significant disruption of same one or more of the organisation's business activities.

Note that production of a BCP is *just one of several required elements* - comprising in total a 'Business Continuity Management System'

.....and another way of saying this:

Business continuity methodology components - produced as a documented plan

- **Business Continuity Policy**

A 'Business Continuity Policy' statement typically sets out the 'higher level' view of:

- An organisation's aims, principles, objectives and approach to BCM in general and introduction of a BCMS in particular
- How, when and in what way(s) the BCMS shall be delivered - including scope
- Definition and documentation of key BCMS roles & responsibilities
- BCMS governance and review

- **Business Continuity 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'

- **Business Continuity 'Requirements / Resources' Analysis**

The process of collecting, documenting and analysing information re all of the *resources* which might be *required* in order to continue / resume business activities (following a significant disruptive event), at a level commensurate with supporting an organisation's declared BC Policy and Strategies





▪ Business Continuity Strategy

Appropriate strategic (higher level / longer term) choices made by an organisation - necessary to ensure (insofar as is possible / practicable / desirable) continued production / operation (possibly following a temporary cessation of same) of its key product / services / operations / activities / tasks etc. (albeit to a potential, pre-defined level of operations - being *below* that of *normal* operations), following a significant, disruptive event

BC strategy is typically formulated as based on the results of (inputs from) the associated 'understanding the organisation' task

Very generally speaking, there are three 'generic types' of BC strategy which might be considered (i.e. choose the most appropriate strategy and expand upon it) with regard to each key product / service / operation / activity / task etc. under consideration i.e.

1. *Be fully productive / operational - **at all times*** (e.g. a trauma hospital)
2. *Produce / Operate / Respond etc. to **pre-defined** (possibly incremental) and acceptable, **minimum level(s)** (see 'Minimum BC Objectives' - **MBCO**) **within pre-defined and acceptable time periods** (see 'Maximum Tolerable Period of Disruption' - **MTPD** / and 'Recovery Time Objective' - **RTO**)*
3. ***Do nothing*** (Pedantically speaking, the 'do nothing' choice is **not** a BC strategy. Rather, it is a **RISK** management strategy / treatment)

Note - within general & current BC terminology, there is a fairly common (and somewhat confusing) intermixed usage of the terms 'BC Strategy' and 'BC Options'. Generally speaking, both terms refer to the same subject - as documented immediately above. However, the term 'BC strategy' is used in *this* guideline document - in preference to the term 'BC Options'

▪ Business Continuity (Tactical) Treatments / Controls

Tactical (operational level / shorter to medium term) measures, taken by an organisation, in order to achieve the requirements of an associated BC Strategy - with regard to a **specific** key product / service / operation / activity / task etc.

- For '**Full Production / Operation**' - the BC 'strategy' will require appropriate BC '**tactical treatments / controls**', which are capable of **immediately** (or as near immediately as possible - given the actual disruption circumstances 'on the day') resuming production / operation of the associated activity etc. post disruption

Examples of such activities include surgical operating theatres; other critical hospital facilities; other critical emergency services; a key main activity which can only be operated via ICT resources (e.g. the website of an 'on-line only' retail organisation); an airline's only 24H call (reservations) centre; a category IIIB ILS at an airport when e.g. 'below normal limits' weather is forecast (and, in fact, most Air Traffic Services in general also 'qualify' here) etc.





All such BC treatments must obviously be 24H ready for near immediate implementation / takeover - and this is generally only achievable via 'hot duplication' i.e. the same key product / service etc. is maintained at all times at a minimum of two different (strategically located from a BC viewpoint) facilities - **OR** perhaps by having * multiple redundant systems etc. Not forgetting the need for 'competent' people to immediately take over operation of such hot backup facility - however this might be achieved

*However, such systems (e.g. a 'no-break' power supply system co-located or very close to where the activity takes place) will be of no use of course if e.g. the associated facility where the activity takes place burns to the ground i.e. the no-break supply should be located well off-site

- For 'option' 2 (see definition of 'BC Strategy' on previous page), appropriate BC 'tactical treatments / controls' are applied in order to deliver what is required. Some typical examples include:
 - An appropriately equipped (resourced) and located 'back-up / alternate' facility (warm or cold) - where staff delivering key operations / services / activities - can be transferred, accommodated and operate at short notice
 - Alternative suppliers and / or the self-storage and rapid availability of identified stock and similar
 - Use of (competent) alternate / interim staff to fill 'empty' posts
 - 'Working from home'
 - Reciprocal (mutual) aid arrangements with similar organisation(s) etc.
- 'Doing Nothing' (strategy 3) - might be regarded as an acceptable BC 'tactical treatment / control' in appropriate circumstances

This latter treatment might be used following a cost / benefits analysis of the BC treatment(s) available to meet a specific BC strategy - and where the conclusion is made that the potential benefit(s) of deploying such treatment(s) are outweighed by the costs of same. Note, however, that there may also be potential adverse implications in 'doing nothing' - if not managed correctly. Such implications typically affect brand, image and reputation type issues; crisis communications; financial matters etc.

Consequently, in choosing this treatment it is important to identify any further potential, adverse impacts which might arise as a result of 'doing nothing' - and pre-establish appropriate counter-measures accordingly - e.g. the need to communicate with stakeholders / other interested parties as to 'why the decision to do nothing' was taken; providing some form of compensation or similar to those disadvantaged as a result of 'doing nothing' (e.g. airline customers) etc.

Note 1 - 'doing nothing' is a good example of a BC treatment which itself potentially creates further risks and associated impacts - leading in turn to the need for further risk and / or BC treatments.....and so on





Note 2 - the term '**BC tactical treatment / control**' is specific to **this** guideline document only. Within general BC terminology around the world it can also be known as '**BC Options**'; '**BC Tactical Responses**' etc. Even more confusingly, '**BC Options**' is also sometimes used to mean the same thing as '**BC Strategy**'

BC tactical treatments / controls are *unlikely* to be applied in isolation - rather, a combination of the most appropriate treatments will typically be applied e.g. for an important (key) activity such as an **airline's** main operations control centre or an **airport's** terminal building management centre - it is likely that some / all of the following would be considered (the list is **not** exhaustive):

- Use of a **fully equipped, relatively nearby** (i.e. a different location) & **ready to go** (WARM) **alternative / backup** facility
- A suitable system for **rapidly reinforcing on-duty staff**
- A robust method of **back-up communications** (e.g. satellite phones, tetra radio [with telephone & messaging capability], smart phones)
- Access to a back-up (off-site) but easily and relatively quickly accessible **repository for information** (*hard copy*) **and data** (*soft copy / electronic info*)
- **Use of cross-trained staff** in appropriate secondary roles
- '**Working from home**' capability for selected staff etc.

▪ **Business Impact Analysis (BIA)**

BIA (taken together with the *other* three components of the '**understanding the organisation**' task [see page 125]) is the foundation of Business Continuity Programme Management. In very brief summary it (BIA):

- Identifies an organisation's **key product(s) / services / operations etc.**
- Identifies **key main activities and resources** (internal & external) associated with delivering the above key product(s) / services / operations etc.
- Identifies **key supporting activities and resources** (internal & external) associated with **supporting** delivery of the above key **main** activities etc.
- Assesses the **prioritisation** (scoring by degree of urgency) of 'key main & key supporting activities' to the organisation, **with regard to their continuity / resumption**, following a significant disruption eventand
- Assesses the **impact over time** of (uncontrolled & non-specific) disruption of such key main & supporting activities - on the delivery of the organisation's key products / services / operations etc.and
- Estimates the timescales (**MTPD** and **RTO**) by which BC tactical treatments for each key main activity and key supporting activity above (individually - **and** in relation to one another where appropriate) must be applied, in order to avoid unacceptable consequences to the organisation's stakeholdersand
- Identifies internal & external dependencies etc. - relating to the same 'key main activities' and 'key supporting activities' and, where appropriate, **adjusts initial RTOs** (*as calculated above*) **to adequately account for same**and





- Sets the minimum level of operation (**MBCO**) to be achieved when a disrupted activity 'resumes' within or by RTOand
- Identifies '*single points of failure*' for any further action.....and
- Uses '*degree / level of adverse impact outputs*' from all / any of above as **one** of the **inputs** to the associated **risk management / assessment** process.....and
- **Pulls together & documents** the results of **ALL** of the above (and more) into a report which, when approved by top management, is used (going forward in the BCPM task) to formulate an associated '**BC Strategy / Strategies**'. That strategy (strategies) will, in turn, outline (from the higher level / longer term viewpoints) what the organisation needs to achieve - in order to try to ensure continuity of its key activities, following a significant disruption event to sameand
- Identifies and accounts for **other** activities which **might** require consideration from a business continuity context - but which are **not** expected to require application of the formal BIA & Risk Assessment processes described above

Note - known / expected seasonal factors e.g. peak trading periods; peak vacation periods for staff; deadlines for submission of legal, regulatory, financial and similar returns / reports etc. must also be factored into appropriate elements of the above

The BIA necessarily focuses on those activities - failure of which would most quickly threaten whatever it is that needs to be operated / produced / delivered. This focus is typically directed to 'operational / high profile / up-front' activities (key main activities - both internal and external). However, many (if not most) of such activities will depend, in turn, on other 'backroom' activities (key **supporting** activities - both internal and external) which **must also** be documented and analysed via the BIA

The BIA can be difficult to perform competently but must be 'got right' if it is to be effective. It can also take quite a long time - depending on the size and / or complexity of the organisation, the scope of the BIA, the co-operation of participants and the competence / experience / availability of the person(s) undertaking the associated data gathering & analysis of same - and, lastly, the degree of top management support

▪ **Business Recovery / Business Recovery Plan**

Whilst Business Continuity is targeted (following a disruptive event) at operating an organisation's activities etc. **to a pre-targeted minimum level of output** (see MBCO) **within pre-targeted timeframes** (see MTPD & RTO) - **Business Recovery** aims thereafter to gradually **restore** such activities etc. to a more sustainable level than that required by MBCO - and eventually to 'normal operation' levels

Note - Business **Recovery** operations are **not** the **subject** of **this** guideline document. Where mentioned herein - it is typically for contextual and / or information purposes only





- **Competence**

The demonstrated ability of someone to adequately apply the knowledge, skills, experience etc. - considered necessary to achieve intended results / goals / targets etc. Competence is achieved via a mix of training, exercising, on the job experience etc.

- **Compliance / Conformity**

Compliance = the extent to which requirements are fulfilled. When a requirement is of a mandatory nature, the word *conformity* is used instead (the latter typically being a component of an appropriate 'modern management system' - as referred to herein)

- **Corporate Governance** (Governance, Risk & Compliance - GRC)

Companies generally direct & control their affairs by using a system of corporate governance - with 'Boards of Directors' typically being responsible for such governance

The 'stockholders / shareholders' role in governance is to typically appoint directors & auditors - and to satisfy themselves that an appropriate governance structure is in place

The responsibilities of the 'board' typically include setting strategic goals, providing the leadership to put the latter into effect, supervising the management of the business and reporting to the stockholders on the board's 'stewardship'. The board's actions are generally subject to laws, regulations, rules, morals and the wishes of stockholders

From a BC / Risk Management viewpoint, corporate governance generally includes a requirement to describe business risks to the organisation, via audited annual reports - together with the appropriate management / mitigation measures put in place to control such risks. In some jurisdictions a board level director assumes responsibility for the organisation's risk management (*including BC*) oversight responsibilities

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

One definition

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

..... & *another*

Important, time-sensitive *activities* (including associated resources, dependencies, inter-dependencies etc.) necessary for an organisation to be able to deliver its key product / services / operations in the appropriate manner prescribed (including the taking of 'Risk Management' type activities)





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 indicated in the two definitions immediately above. However, it should **also** be interpreted (where appropriate) in a different context e.g. of being critical for the purposes of prevention of death or injury - and similar - where time might not be a significant factor

- **Dependency**

Relates to how one activity may depend (for its functionality etc.) on a **different** activity. **Inter-dependency** refers to the same concept - but now where all activities considered (being more than two) depend on each other for functionality etc.

- **Disaster Recovery (DR)**

A term traditionally used to describe the activities, processes and resources dedicated to prevention of an **ICT** failure / significant disruption and, if such prevention proves to be unsuccessful - the application of the appropriate recovery technique(s) to eventually restore 'normal operations'

The term is today much misunderstood and misused - especially outside its ICT context. Use of this term in **this** guideline document will **only** be as described above

Similarly, the term 'business continuity' is often [mistakenly] used today - where 'disaster recovery' would [at least pedantically] be the more appropriate term to use

- **Disruption (Outage)**

Anticipated/unanticipated events which significantly disrupt normal business activities

- **Emergency** (Emergency Response [Plan / Planning]) - (ERP)
- **Crisis** (Crisis Response [Plan / Planning])
- **Incident** (Incident Response [Plan / Planning])



All of the above can and do mean 'all things to all men' - depending on context, historical use, ignorance etc. However, and as used in **this** guideline document, the terms 'emergency' and 'crisis' relate to some form of * **very serious** occurrence and the **initial** (immediate / near-immediate) response(s) to same (e.g. evacuation; fire-fighting and rescue; immediate medical treatment; hospitalisation; provision of humanitarian assistance; provision of crisis related information etc. **BUT - NOT THE APPLICATION OF BUSINESS CONTINUITY MEASURES**)

* For an aviation context 'very serious' typically relates to a catastrophic aircraft accident type scenario or equivalent





Consequences of an emergency / crisis **might** (repeat - *might*) lead on (*eventually*) to activation of (separate) business continuity / recovery type operations i.e. **additional to** the emergency / crisis response itself which, if it (the latter) lasts long enough will need to be operated and managed **concurrently** with any eventual BC response

As an example - a major aircraft accident might be termed an 'emergency' or 'crisis' - and the parent (or related) organisation's initial response typically guided by some type of **emergency / crisis** response plan (Note - '**Emergency Response Plan [ERP]**' is the preferred term used in **this** guideline document)

A greater or lesser degree of **disruption** might typically be associated with such an emergency (e.g. closure of the main airport / airport hub serving the [accident related] aircraft operator), requiring implementation of a **separate business continuity plan** and, eventually, a **separate business recovery plan** - for **both** the accident airline and airport concerned (as appropriate)

Note 1 - within a Business Continuity context / common use terminology, **all** of the above named plans and supporting infrastructure are [**incorrectly & confusingly**] 'lumped in together' as something known as the '**Incident Response Structure - IRS**' - even though what is being responded to might, in fact, be a major emergency / crisis - (i.e. use of the less impacting term '**incident**' in such circumstances can be potentially confusing when used in an aviation context. See also 'notes' starting on page **62** for further clarification on this matter)

Note 2 - in **aviation** related terminology the word 'incident' typically refers to a much less serious occurrence than that associated with the word 'emergency'. 'Incidents' happen relatively regularly within aviation and are usually responded to in a fairly low key manner. They rarely give rise to consequences which require activation of associated (formal) business continuity plans and / or emergency response plans

Note 3 - Important - for medium to larger sized airlines/airports - it is common for 'emergency response' ops and 'business continuity' ops to be **treated separately** i.e. separate plans; separate command & control systems, separate response teams in separate locations; separate resources (to a degree) etc. That said, a significant degree of co-ordination, co-operation and consistency between the two **must** obviously be applied - during the associated planning, training and exercising phases of both - and during actual (real) operations involving both

▪ Establishing the 'Context'

Defining, differentiating & documenting the external and internal parameters / factors (contexts) to be accounted for - when managing business continuity (and also when setting BC scope and criteria for the BC policy):

External Context

Typically includes:

- The cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environments etc. - whether international, national, regional or local





- Other external key drivers (influences) and trends having impact on the objectives of the organisation
- Relationships with (and perceptions and values of) external stakeholders / other external 'interested parties'

Internal Context

Typically includes:

- Governance, organisational structure, roles and accountabilities
- Policies & objectives - together with the strategies in place to achieve them
- Capabilities, as understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies etc.)
- Information systems, information flows and decision making processes (both formal and informal)
- Relationships with + perceptions and values of internal stakeholders / interested parties
- The organisation's culture
- Standards, guidelines and models adopted by the organisation
- Types and extent of contractual relationships

▪ **Gap Analysis**

A survey aimed at identifying differences between 'what is required' - compared to 'what is actually in place'. In the context of this guideline document, the term / concept is typically applicable to an organisation's *Business Continuity* requirements

▪ **Horizon Scan** (See appendix C to this document - starting on page 302)

▪ **Impact**

The (typically adverse) consequence(s) resulting from an inability (for whatever reason) to adequately undertake or fulfil a required business process or equivalent

Note - such impacts can typically include loss of life and / or injury; damage to the physical & social infrastructure of a community; damage to the environment; political, corporate or personal embarrassment; financial loss; breach of law / regulations / standards etc.; failure to achieve agreed service levels; increased costs of working; loss of competitive advantage; loss of credibility; loss of key skills; brand, image & reputation issues etc.

▪ **Incident Response Structure** (IRS)

See notes 1 to 3 on page 34 - and also the notes found (starting) on page 62





- **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..... 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 for a **significant** time / period / duration, might have unacceptable (adverse) impacts on the organisation and / or its stakeholders and / or 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** - key product / services / operations should be documented within the '**scope**' section of an organisation's '**BC Policy**' statement

- **Maximum** (amount of) **Tolerable Data Loss** (MTDL)

The maximum loss of **data / information** (electronic & otherwise [e.g. hardcopy]) which an organisation is able to tolerate (see also 'Recovery Point Objective - RPO')

Note 1 - the age of the lost data could make operational recovery difficult / impossible; **Note 2** - the value of the lost data could be substantial enough to put business viability at risk; **Note 3** - the concept of MTDL **must** clearly be understood. However, this guideline document concentrates, in the main, **only** on MTPD (for more information see 'scope' page 22)

- **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) (AND / OR any associated [subordinate] activity / activities) - **to become unacceptable** to the organisation's stakeholders / other interested parties

An **overarching** (strategic) **MTPD** should be estimated, approved and documented for **each** key product / service / operation - followed by **MTPD** estimations for **each** associated **key main activity** required to produce / operate its associated (parent) key product / service / operation etc.

An **overarching** (strategic) **MTPD** should be estimated, approved and documented for **each** key product / service / operation - followed by **MTPD** estimations for **each** associated **key main activity** required to produce / operate its associated (parent) key product / service / operation etc.

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





MTPDs should then be set, in turn, for *each key supporting activity* required to support the associated (parent) *key main activity*

Note - The estimation 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 and activities

Note 1 - 'subordinate' MTPDs must be equal to or shorter (in terms of time period) than an associated, 'parent' MTPD

Note 2 - 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. **However, in reality, all such processes** (as associated with their 'parent' activities) **must be accounted for** - and any which are considered 'significant' from the business continuity viewpoint are to be assigned MTPDs in their own right

Note 3 - Some typical consideration factors used in estimating MTPDs might be:

- 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
- Potential environmental *damage*
- *Other* potential factors specific to the organisation

Note 4 - the term 'Maximum Tolerable Period of Disruption - MTPD' can be difficult to correlate with its meaning as given above. In fact, it can be downright confusing

Significant debate has occurred (over recent years) amongst the 'professionals' 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 guideline document and is also acceptable to ISO 22301

Unfortunately, it appears (best guess) that 'MTPD' might be used more around the BC world (2018) than 'MAO'. Accordingly and reluctantly, MTPD is also used (usually in conjunction with 'MAO') in this guideline document





- **Minimum Business Continuity Objective(s) (MBCO)**

Pre-planned *minimum, acceptable* delivery levels of an organisation's key product / services / operations - together with their associated, subordinate activities etc. (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.....' (See also Notes 1 & 2 which accompany the definition of 'Recovery Time Objective - RTO')

- **Modern Management System (MMS)**

e.g. Quality Management System; Safety Management System; *BC Management System*; *Risk Management System*; Environmental Management System; Operational Health & Safety Management System; Document Management System etc.

A specific management system - typically being a '*component*' of an organisation's *overall/overarching* management system (see list under title above for examples of such component systems) - which establishes, implements, operates, monitors, exercises, reviews, maintains and improves that particular '*component*'

The key components of a typical modern management system include:

- A *policy* - complete with *objectives & scope*
- Management processes to *support the policy & objectives* - within the scope
- Specific processes to *plan, implement, operate and achieve the policy & objectives* - within the scope - including associated (tactical) *business activities*
- Sufficient *people resources* complete with assigned roles, responsibilities, accountabilities, competencies and skills
- Sufficient *other resources* - e.g. budget, time, facilities, ICT, equipment etc.
- A supporting *documentation system* e.g. plans, reports, records etc.
- Suitable methods of *assessing the performance* of the system +
- Suitable methods of *continually improving* system outputs +
- Periodic *review* of the system by appropriate *senior management* +
- Specified elements of system subject to ongoing *compliance* (audit) *checks*

An MMS typically follows the ISO derived '**Plan → Do → Check → Act** (PDCA)' cycle in order to try to achieve continual improvement in its 'output' and to meet 'customer satisfaction' parameters - whoever the customer might be

Note - the concept of a 'management system' as described above was relatively new (as at 2018). The term 'modern' management system is used in this guideline document *only* - to particularly refer to the above definition and to avoid confusion with any other common interpretations of the term 'management system' e.g. as might be used unintentionally with 'historical / outdated' interpretations





- **Objective**

The end purpose / aim of a process, of an activity, of an organisation as a whole etc. Objectives are typically expressed in terms of *measurable* targets

- **Organisation** (Entity)

As used in this guideline document - an 'organisation' is a generic term depicting any entity to which the concept and practice of business continuity can apply. The scope of this term (as used herein) typically refers to *medium* to *large* sized (and / or complex) entities - unless stated otherwise

- **Policy**

An organisation's intentions & direction - as formally expressed by its top management

- **Procedure**

A *procedure* is a specific way of carrying out a *process* - typically including (at its simplest):

- Who performs what action(s)
- In what sequence the defined steps in the action(s) should occur
- 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 general procedure might comprise a simple flow diagram, a detailed procedure could be a one page form or it could be several pages or more of text / flow diagrams 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
- States which inputs should be used and what outputs should be delivered

- **Process**

Inter-related / interacting operations - using *resources* (one or more of which might 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. use 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** resources do you need to do your work / jobs?

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

Can you explain (provide an overview) **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'?

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, 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

▪ **Process Mapping**

A process map is a 'tool' commonly used to **visually** illustrate (on paper; electronically etc.) work flows. It can also be used as a communication tool, a business planning tool and a tool to help manage an organisation. Key elements include:

- Inputs
- Outputs
- Activity steps
- Decision points
- Functions





Process mapping involves the gathering and organising of facts about the required work - and displaying them in a visual format so that they can be questioned and improved upon by 'knowledgeable' people. It also aids in understanding by abstracting (i.e. using visual 'symbols' consistently) and by masking unnecessary detail

The standard lines and symbols used on a process map (*not included here*) help us to record concise sentences for every step in the process - which tells the user / reader:

- What is happening
- Where is it happening
- When is it happening and how long it will take
- Who is doing it
- What resources are required

Process mapping is used to gain / improve 'better understanding' of a subject - and is typically used in the BC context - as part of the '**Business Impact Analysis**' process

- **Recovery Point Objective** (RPO) (Critical Data Point)

The RPO is the maximum acceptable level of **data / information** loss following an unplanned 'event' (such as a disaster [natural or man-made], criminal act / terrorism, negligence etc.) which could cause such loss. The RPO thus represents the **point in time**, prior to such an event or incident occurring, to which lost data (electronic and / or hard copy) might be able to be successfully recovered (provided that the most recent, planned backup copy [if any] etc. of the lost data is available 'somewhere' of course)

..... & another definition

The pre-planned **target** set for the status and availability of data (electronic and / or hard copy) at the start of a recovery process

See also 'Maximum Tolerable Data Loss' (MTDL)

Note - the concept of RPO must be clearly understood of course. However, this guideline document concentrates **only** on RTO. (For more information see 'scope' page 22)

- **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, in turn, the latter's [associated / subordinate] **key supporting activities** - where appropriate) to a pre-determined level of output (see MBCO) - following disruption

Set RTO too late & the organisation could encounter big resumption problems; set it too early & the associated costs of managing same might easily outweigh the benefits





* The term 'resuming' should not be taken as meaning **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 emergency services & similar etc.

RTOs must always fall within (be the same or earlier [shorter] than) the MTPDs calculated for their associated (**parent**) *key product / service / operation etc.* - *plus any associated key main activities / key supporting activities / supporting processes etc.*

Note 1 - RTO calculations for a particular business activity may, in turn, be dependent on RTOs calculated for one or more **other** business activities - and vice versa e.g. if activity **A** depends for its recovery upon activity **B**, then the latter's RTO must be equal to or less (in terms of time) than the RTO of activity **A**. Any **originally** calculated RTO for activity **B** must be adjusted accordingly if necessary. Where it is not possible to adjust e.g. the latter RTO as described (for whatever reason) then an alternative, acceptable (to the organisation) solution must be found

Note 2 - If an RTO is changed as described in Note 1 above - the associated (existing) MBCO must also be checked to see if it remains appropriate - with regard to such changed RTO

▪ Resilience

The ability of an organisation, system, network, activity, process (etc.) to absorb the adverse impacts of an interruption, disruption, loss (etc.) to its products, services, activities (etc.) - and still continue to provide a minimum acceptable level of same within a desired (pre-planned) timescale (i.e. **business continuity**) - and a return to 'normal operations' ASAP after that (i.e. **business recovery / resumption**)

▪ Resources (BC specific) (Continuity Resources)

An organisation's assets - including e.g. people, skills, information (electronic and / or otherwise), technology (especially ICT), equipment, premises, facilities, supplies etc. - all being necessary in order to meet its declared **business continuity objectives**. Most organisations will need to use at least some resources which require external sourcing

▪ Risk

Evaluation of a specified **threat** (+ the associated **vulnerabilities**) on something / someone (the latter being subject to the threat) - which, when combined with the **impact** of that **threat** (on the something / someone) should it actually occur (be realised) = **the risk** with regard to that something / someone - as related to that threat

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

The considerations of any particular risk can (& should) be based on **both** the projected negative (adverse) & positive (beneficial) **outcomes** (see also 'Risk Appetite')

One (but just one) of several methods used to 'treat' (deal with) risk uses appropriate BC measures (via use of appropriate BC strategies & associated BC tactical treatments / controls)





..... & another definition

Any internal or external situation / event having the *potential* to impact upon an organisation - and which might (if it occurs) prevent the latter from successfully achieving some / all of its business objectives; capitalising on its opportunities etc.

- **Risk Appetite** (see also 'Risk Tolerance')

The *amount* & *type* of risk that an organisation is broadly willing to pursue / retain (accept, tolerate and / or be exposed to) - *at any particular point in time* - with a view to attaining / maintaining / improving 'value' with regard to its business objectives (whatever the term 'value' means to the organisation [when taken in context]). Risk appetite is a product of mission, culture, policy and other factors which determine 'what an organisation is' - and how it goes about its business

For example - BC planning is one (but only one of several) element (treatment / control) of the Risk Management process, designed to ensure that an organisation can continue to deliver its key products and services to clients / customers. The depth of BC planning and measures *applied* depends upon the level of risk and impact on the organisation which it (has considered and) is prepared to accept, as a result of an impacting disruption - *and as predicated on its declared & current risk appetite*

To develop this a little further, risk appetite can typically influence the organisation's choice of MTPD, RTO and MBCO. For example, the larger the risk appetite - the longer the RTO and MTPD timeframes might be **and / or** the lower the target level of continuity operations (MBCO) to be achieved by RTO

Procurement / allocation (*or not*) of resources to mitigate risk is also influenced by risk appetite

- **Risk Category**

Similar risks can be grouped together in categories - e.g. operational, safety, security, financial, reputational, regulatory, strategic, investment, infrastructure, people, technology, knowledge etc. (See also appendix B - page 298)

- **Risk Management** - a process used to:

- **Identify actual** and / or **potential threats** to an organisation's key product / services / operations - and their associated (subordinate) **key main** and (in turn) **key supporting** activities and all associated processes (*Threat Identification*)
- **Estimate the likelihood** (probability, frequency, chance etc.) & potential **degree** (effects, consequences etc.) of the (typically) **adverse impacts** of such threats on the organisation's **key product / services / operations** - & to the associated (subordinate) **key main** and (in turn) **key supporting** activities and (in turn) **associated processes** (*Risk Analysis*)





- Prioritise (evaluate) the **results of the risk analysis** according to an agreed formula (**Risk Assessment**)
- Provide information to enable an associated **risk management control programme / action plan** to be implemented (**Risk Treatments / Controls**)

Note - 'Enterprise Risk Management - ERM' generally only differs from 'conventional' risk management in terms of scope e.g. 'operational' type aviation activities are subject (mandatory) to the Safety Risk management process as a result of ICAO's Safety Management System (SMS) requirements

Should the organisation concerned decide to additionally 'roll out' risk management to the **entire** organisation (i.e. not just those departments / business units related **directly** to aviation [flight] operations) - then this would be known as ERM. See page **300** for more details

..... & another definition

Risk Management is an overall process - comprising sequentially:

Threat Identification - identifies and describes the '**threats**' (and the associated '**vulnerabilities**' whereby a threat might be 'facilitated' to actually occur) **which could affect the successful achievement of an organisation's business objectives**

Note - this might involve use of historical data, theoretical analysis, informed and expert opinion - and consideration of stakeholder's / other interested parties' needs

Threat (Risk) Analysis - used to understand the nature of **identified** threats - and to estimate the potential (typically [but not always] adverse) **impact** level of same - **combined with** the estimated **probability** of occurrence

Note 1 - Threat / risk analysis provides the basis for the next step i.e. risk assessment / evaluation & associated decisions required (regarding associated risk treatment(s) / controls)

Note 2 - Threat / risk analysis typically involves some form of personal 'estimation' - which is necessarily 'subjective' by nature - to a greater or lesser degree

Risk Assessment / Evaluation - used to compare identified risks with the organisation's **defined risk criteria / risk appetite** - in order to determine whether or not a specified level of risk is acceptable / tolerable - and to assist in the selection of risk treatments (controls) **which might be employed to manage each identified risk - where required**

Risk Treatments / Controls - any risk assessment results considered '**unacceptable / not tolerable**' will require application of appropriate risk treatments (controls) - to the extent that (in one way or another) the risk becomes acceptable. Where the latter is not possible the risk will need to be removed - which will probably have the knock-on effect of cessation or modification of the associated activity / process etc.





..... & one more definition

Risk Management (RM)

The culture, (supported by associated processes, structures and resources) put in place by an organisation, to effectively manage potential opportunities and risks - based on the declared and current 'risk appetite' of the organisation

As it is not possible (or desirable) to eliminate **all** risk, the objective is to implement cost effective processes which reduce risk to an acceptable level **AND / OR** to reject unacceptable risks **AND / OR** to treat risk via financial interventions i.e. transfer the risks to insurance organisations or similar - **AND / OR treat risk by organisational interventions, one of which may be accomplished by the use of appropriate BC treatments / controls / measures**

▪ **Risk Register**

A comprehensive, documented list of organisational risks by category (graded according to probability of occurrence and related potential [typically {but not always} adverse] impacts) - to which appropriate risk treatments / controls etc. **might** be assigned

▪ **Risk Treatments**

There are typically five **treatments** (controls) which determine how **threats** to an organisation's key product / services / operations / key activities etc. can be 'risk managed' (modified) - in order to eliminate or reduce the associated probabilities of such threats occurring and / or if they do occur, mitigating the associated impacts

1. **Avoidance** - exiting (or not even starting) activities giving rise to unacceptable risk
2. **Reduction 1A** - taking action to prevent / reduce the **likelihood** (probability) of risk occurrence
3. **Reduction 1B** - taking action to reduce / mitigate the **consequences** of 'realised' risks i.e. plan to manage / 'treat' the **impact**(s) of risk after it has actually occurred. One (but only one of several) methods of achieving this is by use of appropriate **BC measures**
4. **Transfer** and / or **share** (all or a portion of) the risk e.g. via insurance; partners; suppliers etc.
5. **Accept** - i.e. take no action e.g. due to 'acceptability' of the particular risk; due to result of a cost / benefit analysis; due to organisation's declared risk appetite etc.





For the purposes of this guideline document only - sub-paragraph 3 above generally relates to the use of *business continuity measures* (treatments / controls). The latter provides for appropriate BC '**tactical treatments**' which might be suitable for use in achieving the desired risk mitigation measures. Choice of which to use, when, how, in what circumstances and by whom - are collectively decided by formulation of associated BC '**Strategies**'

- **Risk Tolerance**

Risk tolerance represents the application of 'risk appetite' to *specific objectives* i.e. whilst *risk appetite* is typically a broad, strategic concept - *risk tolerance* applies within the tactical / operational (hands-on) level of achieving what is necessary

Typically, specific 'objective based' risk tolerances permit the appropriate department (and / or business unit and / or individual) a degree of 'flexible (tactical / operational) risk taking variance' in achieving the specific objective, whilst remaining within the organisation's declared, current & overall (strategic) risk appetite

Risk tolerance measures require pre-approval, documentation, communication and regular monitoring / review

- **Significant**

A generic term (defined here for the purposes of this guideline document only) - meant to convey that 'whatever' it is that is considered *significant* (typically the potential and / or actual consequences [impacts] of disruption on an organisation's activities, processes, resources etc.) is serious enough to require analysis and assessment from the BC viewpoint - and 'acted upon (treated / controlled)' in some appropriate way - if the (BC) circumstances so require and permit

- **Single Point of Failure - (SPOF)**

An activity which depends on a single resource (including a person where appropriate) - which is **not** replaceable should it become unavailable for whatever reason. Such unavailability invariably causes disruption of the associated activity / process etc.

- **Societal Security**

Societal Security refers to protection of 'society' from the effects of incidents, emergencies, disasters etc. - caused by intentional and unintentional human acts, natural hazards, technical failures etc. ('Protection' as used here also includes an active 'response' element e.g. emergency / crisis response operations)





Societal security standards (of which ISO 22301 & ISO 22313 are typical examples) are expected to include the following subject areas (from a societal security aspect):

- Security
- Risk
- Preparedness & Resilience
- Crisis & Emergency
- **Business Continuity**
- Others to be advised

▪ **Stakeholders** (Other Interested Parties)

A person, group of persons, organisation(s) and / or system(s) who / which can affect **AND / OR** be affected by (actually or perceptually) - a decision or activity

The more obvious stakeholders for most organisations include shareholders, clients, customers, suppliers, employees, employee unions, governments, regulators, financial investors, banks, insurers, auditors, professional bodies etc.

Less obvious stakeholders include competitors, the community (permanent & transitory), the organisation's operating environment, the media, protest groups etc.

Note - ISO 22313 uses the term '*other interested parties*' instead of the more specific term 'stakeholder'

The intent of the ISO term is to include **all** elements having an interest(s) in an organisation and vice versa e.g. those listed in the second paragraph above generally fall under the generally accepted concept of 'stakeholders' - whereas those in the third (last) paragraph might not. ISO 22313 bundles them collectively together under the term 'other interested parties'

Where the term 'stakeholder' has been used in this guideline - it will generally have the same meaning as the term 'other interested parties'

▪ **Stakeholder** (Other Interested Parties) **Analysis**

A 'business tool' which can be a useful starting point in the essential '*understanding the organisation*' task - the latter being an essential requirement when introducing and implementing BCMS into an organisation

The analysis quite simply requires a brainstorming session(s) to identify all possible stakeholders / other interested parties associated in some way with the organisation - and then placing them in an initial, listed order of importance (related to what they **expect** from the organisation and vice versa - such expectations also being listed alongside the associated stakeholder / interested party)

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** ('scoring' by degree of urgency with regard to continuity of operation) the organisations **key products / services / operations** etc. (together with associated key main and key supporting activities [+ associated processes] and their inter-relationships, inter-dependencies, resource requirements etc.)

- **Supply Chain**

A series of linked processes beginning with the acquisition of raw material - and ending with the delivery of product / services / operations to an end user (customer). The supply chain may include vendors / retailers, manufacturers, logistic services providers, distributors and distribution centres (internal and external), wholesalers etc.

- **Threat**

Something bad / very undesirable etc. which **might** happen (to something, someone)

- **Top Manager / Top Management**

An organisation's most senior manager / an organisation's top management team e.g. Board of Directors. Where the scope of a BCMS does **not** include the entire organisation - then the 'top manager' will generally be the most senior person in overall charge of each of the organisation's departments / business units which **are** subject to (within the scope of) the BCMS

- **Understanding the Organisation**

A traditional (but possibly confusing) business continuity term which, in 'plain speak', refers to the following 'building block' activities, which need to be accomplished during the early stages of the '**DO**' element of the '**PLAN, DO, CHECK, ACT**' cycle - when introducing a BCMS into an organisation:

- Stakeholder (+ Other Interested Parties) Analysis
- Business Impact Analysis (BIA)
- Risk Management / Assessment (RA)
- Business Continuity Requirements - Resources Analysis

When the above have been completed and analysed, the results may be used to set '**BC Strategy**'

- **Vulnerability**

Exposure to a **threat(s)** e.g. fire is a **threat** to a facility. Associated **vulnerabilities** which might enable this particular threat to be realised (to actually happen) include no alarm system; no fire extinguishers; no other fire suppressant system(s) (e.g. sprinklers) etc.





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

Deliberately Blank





Section 2 / INTRODUCTION

A quick (but very relevant) look at - 'what business continuity is all about'

Please see <http://www.youtube.com/watch?v=DDS833zadfi> before starting this Section 2



Extract from the 'Vikings'
Business **C**ontinuity **P**lan
- Circa 810 AD (CE)



Key Product:	Ravish & Pillage
Key Resource:	Longboat Sail(s)
Threat:	No Wind
Impact:	Unacceptable business loss
BC Treatment:	Use Oars
MTPD / RTO:	Immediate
Resources: 1)	Manpower
2)	Oars
3)	Whips
4)	Luck!





Evolution of BC

The concept and practise of business continuity (BC) is both relatively new (say the last 40 years or so) and something dating back to the beginning of mankind. 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, most early hunters eventually became hunter / gatherers, in order to take care of the possibility that what was being hunted might not be available (temporarily or permanently). In turn, as many hunter / gatherers turned to farming - the need for water outside of any rainy season gave rise to use of e.g. wells, dams and irrigation systems

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 the oars

However, it is only in the very recent past (i.e. with the evolution of information & communications technology - say from about the mid-1980s) that BC has come to be regarded 'by some' as a professional discipline in its own right - similar to quality and risk management

The origins of modern BC lie in traditional *emergency / crisis* response management and the relatively newer areas of *risk management*, *quality management* and (ICT related) '*disaster recovery*' - particularly the latter. Relatively recent emphasis on 'Corporate Governance' (Governance, Risk & Compliance - GRC) has also increased the importance of BC, whatever the nature of the organisation which is subject to the corporate governance

It is important to note that BC does not replace its allied (but different) disciplines (emergency / crisis response; risk management; disaster recovery etc.) - but should, rather, be accomplished *in conjunction with them* - where appropriate

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 such as fire, flood, sickness, industrial action, denied access to facilities & information, information loss etc.

Taken separately or together, 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 for an organisation - and even failure (of the organisation) in extremis

* Note - the meaning of '*unacceptable*' will need to be decided (put into context) and defined by the organisation itself





Effective, efficient and timely BC intervention can assist in prevention and / or impact reduction (mitigation) of such unacceptable consequences. As such, BC can be an asset to any organisation - and it is worth noting well that whilst BC might be considered to be an intangible asset - like any asset it has worth / value (top managers will like that!)

Introduction of BC practices (e.g. via a 'business continuity management system') into an organisation not only assists in protecting the organisation from potential damage / failure - but can also contribute to the 'bottom line' (increased profit; enhanced reputation etc.) e.g.

- Lower insurance premiums and / or wider insurance cover
- Ability to increase profit margins to customers / clients due their increased confidence in the viability of the organisation
- Increased share price following e.g. successful handling of a major disruption occurrence
- 'Preferred supplier' status
- Advantageous risk taking etc.

It is important at this point to also clearly understand that BC is not necessarily a 'voluntary' concept, i.e. at the whim of organisations as to whether they adopt it or otherwise. See boxed case study (example) at the bottom of page 83 for some further clarity related to this matter





Business Continuity at its Simplest

We have already seen above that 'Business Continuity' (or whatever more appropriate term we might wish to use instead) 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 all areas / types of business, commerce and public sector equivalents

However, the modern evolution of BC over the last 30 - 40 years or so into what some 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 organisations

Indeed, for the vast majority of smaller and medium sized organisations and for a significant number of the 'simpler' larger organisations, modern BC remains a fairly simple process and can be effectively and efficiently applied without many of the complexities referred to above

It is 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 and an undesirable air of 'mystique' - which reinforces the lack of interest factor. All of this is unfortunate because it can lead to many organisations - capable of easily and relatively cheaply introducing *simple* BC measures into their products, services or activities - choosing not to do so

However, we *do* need to go some way into the more complex aspects of BC in this guideline document - so that the user / reader might be more adequately prepared for further training and experience requirements if appropriate, typically as related to the 'professional' application of modern BC within an organisation e.g. in an airline or an airport or a GHA etc. BC related employment capacity

The latter might typically be related to appointment e.g. as both the Flight Safety Manager *and* the Business Continuity Manager for your airline; e.g. being appointed as both the Quality Manager *and* Business Continuity Manager at your airport; e.g. (and, if your airline / airport etc. can afford and / or desires it enough) - being appointed *sole* Business Continuity Manager with no other role sharing

But for the moment, let's see how *relatively* simple BC can be by looking at the very basic steps required to introduce and implement a typical, simple BC system / programme into an 'average' small to medium sized organisation. Refer to the 'abbreviations & glossary' sections found near to the front of this guideline where necessary. Should you get frustrated at the relative complexity of BC as documented *later* in this guideline document - just return here from time to time get a check on reality and perspective!

Step 1

- Identify & document the organisation's *key* * *product(s) / services / operations*. Estimate, agree & assign a *Maximum Tolerable Period of Disruption* (MTPD) to each - based on the organisation's strategic (overarching / longer term) business objectives





* 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..... and so on

For an **airport** operator - *key services / operations* might include providing passenger and cargo related services to aircraft operators; provision of 'duty-free 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 same for **aircraft** operators include provision of aircraft; provision of operating crew; network operations services such as flight despatch and flight-watch; reservations and customer services; aircraft maintenance services; fuelling services; ground handling services; safety & security etc.

Examples for **airport** operators include air traffic control; required availability of runways, taxiways, aprons, aircraft parking; provision and maintenance of navigation aids; ramp & passenger terminal services; departure operations; baggage handling; safety & security, arrival operations etc.

Many **key main activities** will rely, *in turn*, on a number of associated **key supporting activities** e.g. HR services; IT services; financial, legal & insurance services; in-flight catering services; airport car parks etc.

Step 2

- Identify & document **each** **key main activity** and its **associated key supporting activities** referred to immediately above, and then differentiate & document (with reasons and in order of 'urgency' related priority) those considered by the organisation to be **critical** and / or **critically time-sensitive** (i.e. being *critical* in the BC context)
- Do the same (separate list) for all other **key main** and **key supporting activities** - considered to be **non-critical** and / or **not critically time-sensitive** (i.e. **not** critical in the BC context)

(Also include in this step 2 any supporting **processes** which might require similar consideration)

Step 3

- For each (i.e. one by one) identified critical and / or critically time-sensitive activity found in Step 2 - **conduct an analysis** aimed at understanding and documenting the likely, adverse **impacts** on the organisation - should operation of same be unintentionally **disrupted** (for whatever reason) for a **significant** period of time i.e. classify in terms of high, medium or low adverse impact (Note - the meaning / context of 'significant duration' will be decided & documented by the organisation)
- **List these impacts in descending order of (adverse) severity** i.e. the most severe being at the top of the list. Where adverse impacts are judged to be similar for an activity - the organisation's top management should decide their relative position on this list





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

Note 2 - Associated **MTPDs**, **RTOs** & **MBCOs** would be estimated, agreed & assigned i.e. as applicable to the critical and / or critically time-sensitive activities obtained via Steps 2 and 3 above. For the sake of clarity, this has **not** been done in this simplified example. Note that such RTOs must fall within the declared MTPDs for the (associated) activity in question

MTPDs for key **supporting** activities should be equal to or less than the MTPD set for the **associated** (parent) key **main** activities - and the latter MTPDs must, in turn, fall within the MTPD for the **associated** (parent) **key product / service / operation** - as decided in Step 1

IMPORTANT REMINDER - business continuity planning matters concerning data (both soft and hard copy) loss / recovery are outside the scope of this guideline document - but must nevertheless be accounted for in reality

Step 4

Conduct a '**Risk Management / Assessment**' - by identifying & documenting all actual or potential **threats** which might realistically cause disruption to **each** critical / critically time-sensitive activity (as found and listed in step 3 above)

During this assessment some form of (necessarily subjective) 'scoring system' is used to **estimate** the **likelihood** (*probability*) of each considered threat **actually occurring** when set against what the organisation 'does' (what is the nature of its business)

The **level** (severity) of **impact** of **each** considered threat on **each** considered activity (should the threat be realised [i.e. actually occur]) is also assessed. The results (coming from this para and the one above) are documented - typically in a document known as a '**Risk Register**'

Note 1 - within the BC context the 'assessment of impact' information comes from Step 3 above

Note 2 - For an example of a risk(s) register (this one at national [country] level) - follow the below link:

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

Step 5

The results from Steps 3 & 4 are used to create a series of '**Risk Matrices**' - one matrix per **each** identified critical / critically time-sensitive activity (*as documented in Step 3*) and its associated and relevant risk(s) (*as documented in Step 4*). The estimated level of **impact** for that particular risk (on that particular activity) is positioned along one matrix axis - and the **likelihood** (*probability*) of that risk occurring (to that particular activity) along the other axis

See figure 1 diagram page 57 for a **very** simplified example of a risk matrix





Step 6

By analysing information derived 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 e.g. complete failure of an organisation's electricity supply for a significant period of time) is to plan to **manage** the particular risk **after** it has occurred - using *Business Continuity strategies and associated BC tactical treatments / controls - together with associated BC plans & procedures etc.* - and it is mainly this latter subject which you will be studying in this guideline document

* Note - see 'Risk Treatments' in Glossary - for a full list of choices

Two examples of what the 6 steps shown above are meant to achieve are shown below:

A small organisation's key staff team win the national lottery and immediately quit their jobs

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

Using an airline related example - there is a very real (high probability) **threat (risk)** of 'server meltdown' resulting in very slow webpage loading (or even the complete inability to access such webpages) associated with the airline's main customer interfacing website - e.g. due to the massive increase in hits following a major aircraft accident to that airline

Typical (tactical) **business continuity treatments** might include having (**pre**-established, resourced and implemented) additional server capacity which can be activated at very 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



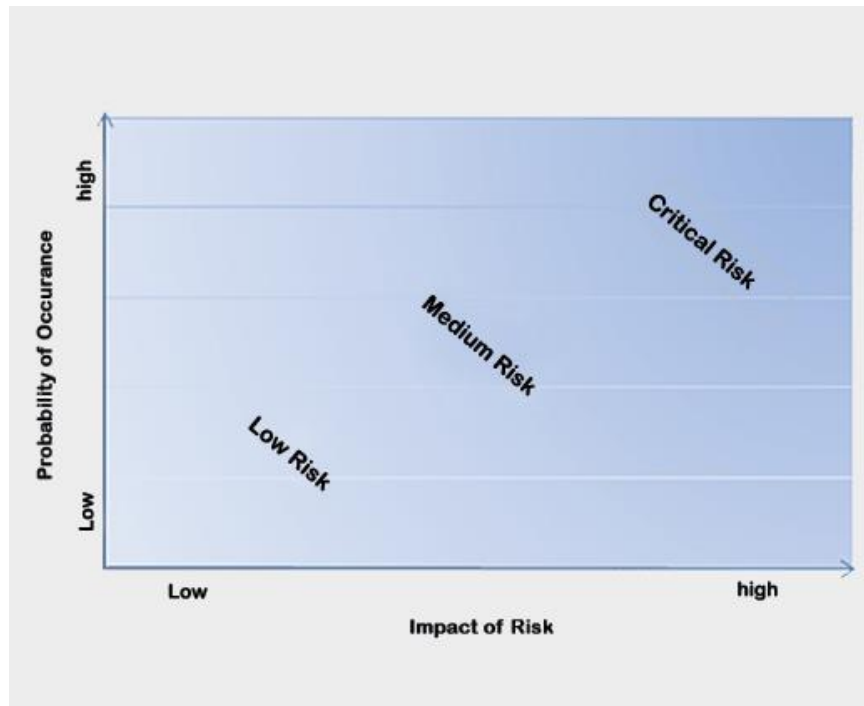


Figure 1 / Simplified Risk (Threat) Probability versus Impact Matrix / Graph

The corners of the above matrix chart have the following risk characteristics relating to any selected critical item obtained from step 3:

- **Bottom Left** - *Low impact / Low probability* - Low level and typically ignored
- **Top Left** - *Low impact / High probability* - Such a potential risk is going to materialise fairly frequently but will generally be able to be handled sufficiently well - probably using just 'normal business' type techniques and resources. However, reasonable measures should *still* be considered 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. Appropriate measures should be taken to reduce (mitigate) the potential, adverse impacts - and a viable business continuity solution (plus other appropriate measures if deemed necessary e.g. an emergency [crisis] response plan) **should be put in place - just in case they do materialise** (A catastrophic aircraft accident is a typical example scenario for **this** particular eventuality)
- **Top Right** - *High impact / High probability* - These risks might be classed as 'critical' and must be dealt with as a top priority

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* - particularly in current media focused times where, if such risk eventuates, **immediate and effective** crisis communications management by the organisation will be a necessity - in addition to any other response methods taken





Step 7

Implement the decisions (make it happen) made in Step 6 - including provision of a supporting and appropriate response infrastructure, 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 2 above

Whilst these may not be 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 probably not be applied to such activity should significant disruption of same arise. However, some response *should* be pre-considered e.g. this might be as simple as maintaining a contact list of nearby fast food outlets which deliver - or asking staff to bring their own food requirements to work

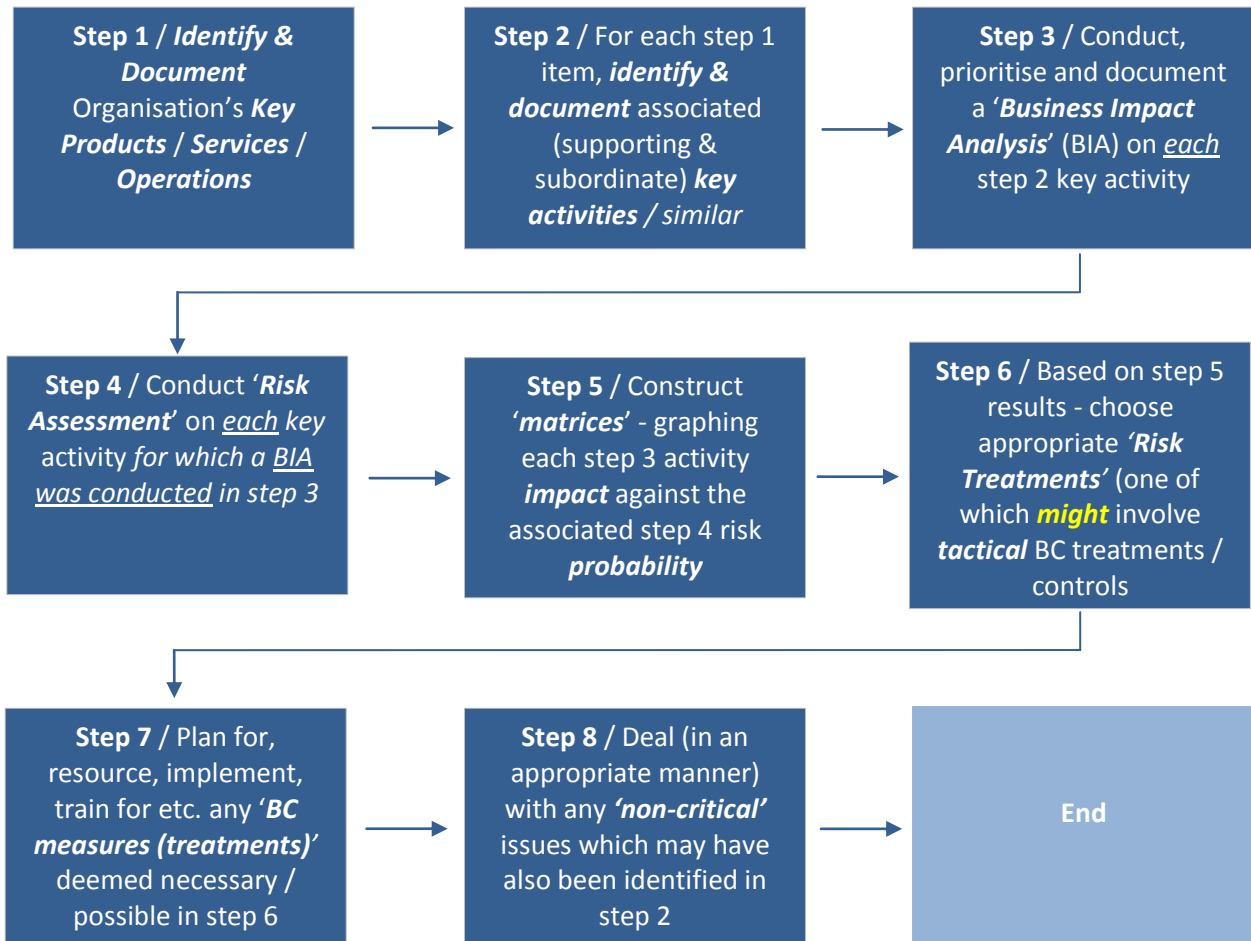
Steps 1 to 8 are shown in simple flow diagram format on the next page

Reminder - the above is merely a *very simplistic* overview and this context should always be considered when studying these 8 steps - and also what follows in this guideline document





Simplified flow-chart indicating the basic steps required to introduce and implement a typical, basic BC system / programme (BCMS) into the 'average' small to medium sized organisation





Is Today's 'Business Continuity' Unnecessarily Complex?

Having now seen how *relatively* simple BC can be, it is worth contrasting here for a moment what might arguably be termed the 'unnecessary complexities' associated with most of the current BC standards, other guidance material and similar - intended to guide us through the process of introducing BC into an organisation

As an example, let's take ISO 22313 (Guideline Standard for how to achieve its associated ISO 22301 requirements). When ISO 22313 was issued as a 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 is probably (and unnecessarily) rather difficult for the layperson to understand and might possibly 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 now reading) has tried (arguably not very successfully) to use wording consistent with the average layperson user / reader having perhaps at least a better chance of grasping the meaning of such wording at first or second reading - particularly if combined with an appropriate training course based on *this* guideline document (such training or similar being highly recommended [*probably essential in fact!*])

Nevertheless, it is readily acknowledged that the wording used in this guideline document itself will also (at least in places) not be as clear and simple as might be desired in order to cater for the 'average' user / reader - especially the non-native English speaker

Accordingly, feedback on how such wording may be further clarified / simplified will be gratefully received (see 'Note 10' on page 10 for further details)

Reminder - the above comments are based on the author / owner's personal thoughts, and he duly acknowledges here that many readers (especially 'BC professionals') will disagree with him on this matter





Potential Benefits of BC

Even if an organisation never experiences serious disruption (and in the nature of disruption it can really still be down to chance rather than effective management), application of the various *BC techniques / programmes / management systems etc.* - can assist in identifying key products / services / operations etc. + associated (subordinate), critical component activities

They (*BC techniques, supported by risk management techniques etc.*) also help to identify and prioritise the adverse impacts of disruption, together with provision of a list (register) of the main risks + the probability of their occurrence. This enables the organisation to be better prepared for the worst and to take associated steps (if it wants to) in order to improve its resilience

Other benefits of introducing & implementing BC in an organisation typically include:

- Reputation / brand / image can be 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 and shares (the opposite also applies of course)
- Compliance and assurance with the expectations of legislators, regulators, insurers, business partners & other key stakeholders / interested parties
- Improving business resilience
- Being an excellent mechanism by which to manage the 'supply chain' and identify any associated weak links in this area - as well as maintaining the confidence of suppliers
- Improving understanding, monitoring & management of risk (including the possibly beneficial applications of 'risk appetite')
- Competitive advantage opportunities - as compared to competitors not embracing BC
- Financial benefits due identification and rectification of organisational weaknesses e.g. single point(s) of failure, duplications etc.
- Adverse financial impacts minimised when disruptions *do* occur
- Information / data assets secured
- Reduced insurance premiums / wider insurance cover / less onerous excesses
- Essential services maintained during disruption - hence customer service (meeting customer requirements) and probably customer loyalty is retained. (This is marketable of course and can be used to retain current customers & attract new ones)
- 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 (especially amongst staff). This can be especially useful in eliminating weaknesses and 'single points of failure' which might have been missed during the BIA - and can also contribute to improved processes, resilience and staff job satisfaction / morale
- Job security improved via the creation / continuance of a sustainable organisation

Note - this list is not exhaustive. It is slanted more towards the private sector than the public sector





Wish-list of BC Outcomes - Cross Reference - ISO 22313 / 8.1.5

Now might be a good time for the user / reader to become aware (in general terms at least) of what (according to ISO 22313) successful introduction of a BCMS into a typical medium to large sized organisation might address 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. Refer to the Glossary where necessary:

- ✓ *Top-management fully 'on-board'* - insofar as BC matters are concerned
- ✓ *From BC viewpoint / context*, the organisation's requirements *to fully understand 'itself' internally* - together with a similar understanding of the context & details of *how it will need to interact and inter-relate with all appropriate external 'interested' parties* - has been adequately researched, developed, documented, understood, accounted for, trained for, exercised for etc.
- ✓ *Supply chain* (if appropriate) adequately *secured*
- ✓ A fully functional '*incident response structure*' is in place - ready to deal with the *immediate* consequences of whatever was the initial cause of a disruption if appropriate (i.e. direct emergency / crisis response) - and to then go on to handle any associated (but separate) *business continuity* and *business recovery* issues - as required

IMPORTANT NOTE - from author / owner of this guideline i.e. the document being read now

See also appropriate, related definitions found in glossary pages 33 to 35 - 'Emergency Response' / 'Crisis Response' and 'Incident' etc. '**Incident** Response Structure' is an '*official*' BC term which is, unfortunately, subject to misinterpretation / confusion - *particularly if used in an aviation context* - where the term 'incident' is specifically & internationally (ICAO) defined (and is typically *not* directly related to BC Ops at all)

The intended meaning of this term *in the BC (ISO 22313) context* covers *all* of:

- The *initial & on-going operational response* to '*whatever it was*' that *also* (sooner or later) causes associated disruption to operations (e.g. a catastrophic aircraft accident 'on-airport' - together with activation of associated *emergency / crisis plans* [but *not* {i.e. at least not yet} *business continuity plans*]).....**PLUS**
- Application of associated business *continuity* measures where required.....**PLUS**
- Application of associated business *recovery* measures where required.....**PLUS**
- Any other response required e.g. 'humanitarian / welfare assistance' measures' communicating with the media and other stakeholders (crisis communications) etc.

However, this BC meaning is incorrect in most contexts (*particularly the aviation context*) as *emergency / crisis / incident response* (as per first bullet point above) is a totally different discipline in its own right and (generally speaking) does *not* consider business continuity matters, except for those required to support its *own*, specific functioning during *actual* emergency / crisis response operations (e.g. ensuring that water supply to responding fire and rescue crews is maintained)





In the aviation context the 4 bullet points shown on the previous page (which, taken together in the *BC context*, comprise the 'incident response structure') **would not be recognised**

Instead, the items covered in the first and fourth bullet points would be known by airlines as the **ERP** ('emergency response plan' or similar term) - and by airports as the **AEP** ('airport emergency plan' or similar term). The items covered by the second and third bullet points would simply be known as the 'business continuity plan - BCP'

Aviation related **ERPs** / **AEPs** are 100% **different** from aviation related **BCPs** - typically having **different** command & control systems; operating from **different** facilities with **different**, responding teams; **different** documentation / checklists etc.

It is suggested that a more appropriate term for 'Incident Response Structure' (as used in the BC context) might be 'Contingency Response Structure' or similar. However, as the former term is currently (2018) in widespread use in the BC context, **it has been retained in this guideline document** (i.e. the one you are now reading)

Nevertheless, the '**aviation**' type user / reader should always keep in mind the '**real / actual / intended**' meanings of the various terms described above - and interpret / act on them in the correct manner accordingly

- ✓ Fully functional **business continuity** and **business recovery** plans and procedures in place - which have identified the organisation's key products & services, have been designed to protect the latter (from disruptive risk) insofar as is desired / possible / practicable - and **post-disruption** will assist in **returning the organisation to normal operations** without undue delay
- ✓ **BC is adequately resourced** - including adequate finance, manpower, facilities etc.
- ✓ **BC awareness, competency and exercise programmes fully established** - 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
- ✓ **Financial controls are maintained** throughout a BC related occurrence
- ✓ **BC performance consistently reviewed and evaluated** via appropriate, on-going (documented) processes. Associated (documented) reports and records maintained
- ✓ **Continual improvement** (on-going) of the BCMS is evidenced and documented

*For a further 'dose of reality' related to users / readers with an **airport** background (and might be of interest to aircraft operators [airlines] also) - have a look at the information found at the end of the below link. The article was written in 2011 (nothing much had changed by 2018!)*

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





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

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 - used as a high level 'road map type tool' to (the planning, developing, establishing / implementing, operating, maintaining, training, exercising, monitoring, reviewing and continually improving) of an organisation's BCMS

As a concept, the PDCA cycle has, as its ultimate aim, the achievement of continual improvement, leading in turn to continually increasing 'customer' satisfaction - whoever or whatever the customer might be:

Plan = **Pre-plan & develop** BC requirements, policy, objectives, targets, controls, processes, activities, procedures, resources, dependencies etc. (**inputs**) - appropriate to establishing, managing, operating and improving BC in an organisation - in order to deliver the required **outputs** (BC outcomes) - as aligned with the organisation's overall BC policies & objectives

Do = **implement & operate** the BC policy, strategies, plans, processes, procedures, activities, treatments etc.

Check = **Monitor & review** BC performance against BC policy, objectives and practical (real life) experience (feedback) of BC 'in action'; present results for review by top management and determine, authorise and enact all remedial measures required to achieve continual improvement - thus continually improving customer satisfaction

Act = **Maintain & improve** the BCMS by use of the 'corrective / * preventive action' system - as 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

* Note - In this document (and in ISOs 22301 & 22313) '**preventive action**' is actually covered as an integral part of the '**risk assessment**' process. Accordingly, the latter term is now generally preferred to the former, provided that its 'preventive action' element is still clearly understood. However, the intent & desired outcomes remain unchanged - and for the purposes of this guideline document only, the terms can be considered interchangeable when used in the appropriate context

The PDCA cycle operates *indefinitely* via the on-going **programme management** (otherwise known as the 'BCMS life-cycle') of its associated BCMS - e.g. there will always be new or revised policies and objectives; targets and controls will change; maintenance is a constant requirement - as are training, exercises, monitoring and review; threats will come and go etc.



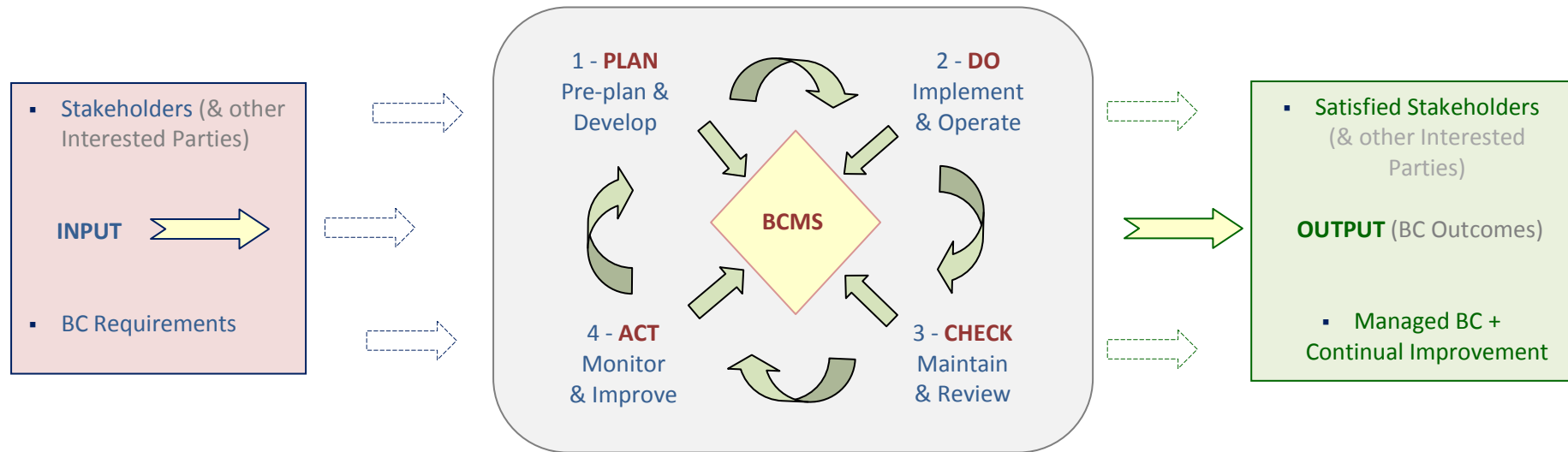


Figure 2 / PDCA Cycle as related to a BCMS



Note from author / owner of this Guideline Document

It is the author / owner's opinion (subjectivity acknowledged) that ISO 22313 is **not** 'laid out' in a manner which sequentially follows the 'PDCA Cycle'

In contrast, the guideline document that you are now reading **does** generally follow this cycle - e.g. as can be evidenced from the titles and content of each of its 'sections' - starting with

Section 4 / 1 page **73**

Note further that the section and sub-section etc. numbering used in **this** guideline document does **not** accordingly follow the same clause and sub-clause etc. numbering used in ISO 22313. However, full cross-referencing to the latter **is** generally provided

Typical **Core** Elements of BC Programme Management

(Reminder - BC Programme Management is otherwise known as the 'BCMS Life-cycle')

Cross Ref - ISO 22313 / 8.1 / 'Elements of a BC Programme'

The BC **Programme Management** elements diagram on the **next** page portrays the **core** elements - as described later in this guideline. An objective here is to try to ensure that the user / reader acquires an understanding of the meaning & application(s) of each labelled element - both individually and as related to ***** other (sub-core) elements, as appropriate

***** Note - Each core element is, in turn, made up of **sub-core** elements - a representative list of the latter being shown in the diagrams shown on pages **70** & **71** of **this** guideline document

Note - from this point on in this guideline document, the PDCA cycle, as it applies in turn to each labelled element of BC programme management (see diagram next page), should be considered to be continually applied - for as long as the BCMS is used within the organisation

Reminder: (Definition)

- **Business Continuity 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'**



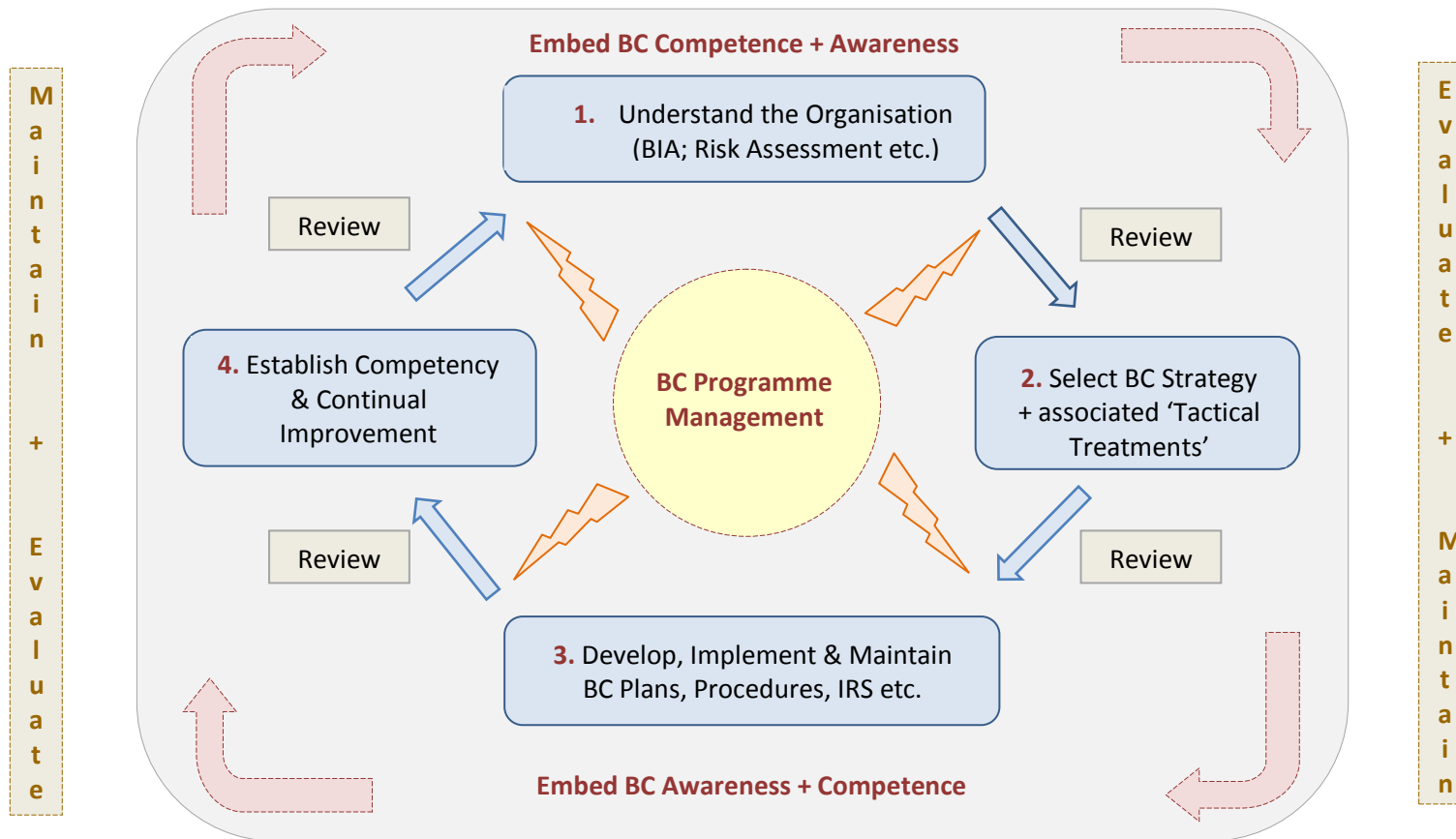


Fig 3 - Typical 'core elements' of a BC Programme (otherwise known as the 'BCMS Life Cycle')



Note 1 - 'Embed Awareness & Competence' in an organisation refers to the on-going tasks of:

- *Top Management* 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 'understanding the organisation' - see page [72](#)

Note 3 - differing terminology for the BCMS lifecycle (than that shown in the diagram on the previous page) may be used in some organisations / standards / documents e.g. (typically):

- 'BC Programme Management' may alternatively be termed '*BC Policy and Programme Management*'
- 'Understanding the Organisation' may be alternatively termed '*Analysis*'
- 'Selecting BC Strategy, Tactical Treatments etc.' may be alternatively termed '*Design*'
- 'Maintain, evaluate and review' may be alternatively termed '*Validation*'





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

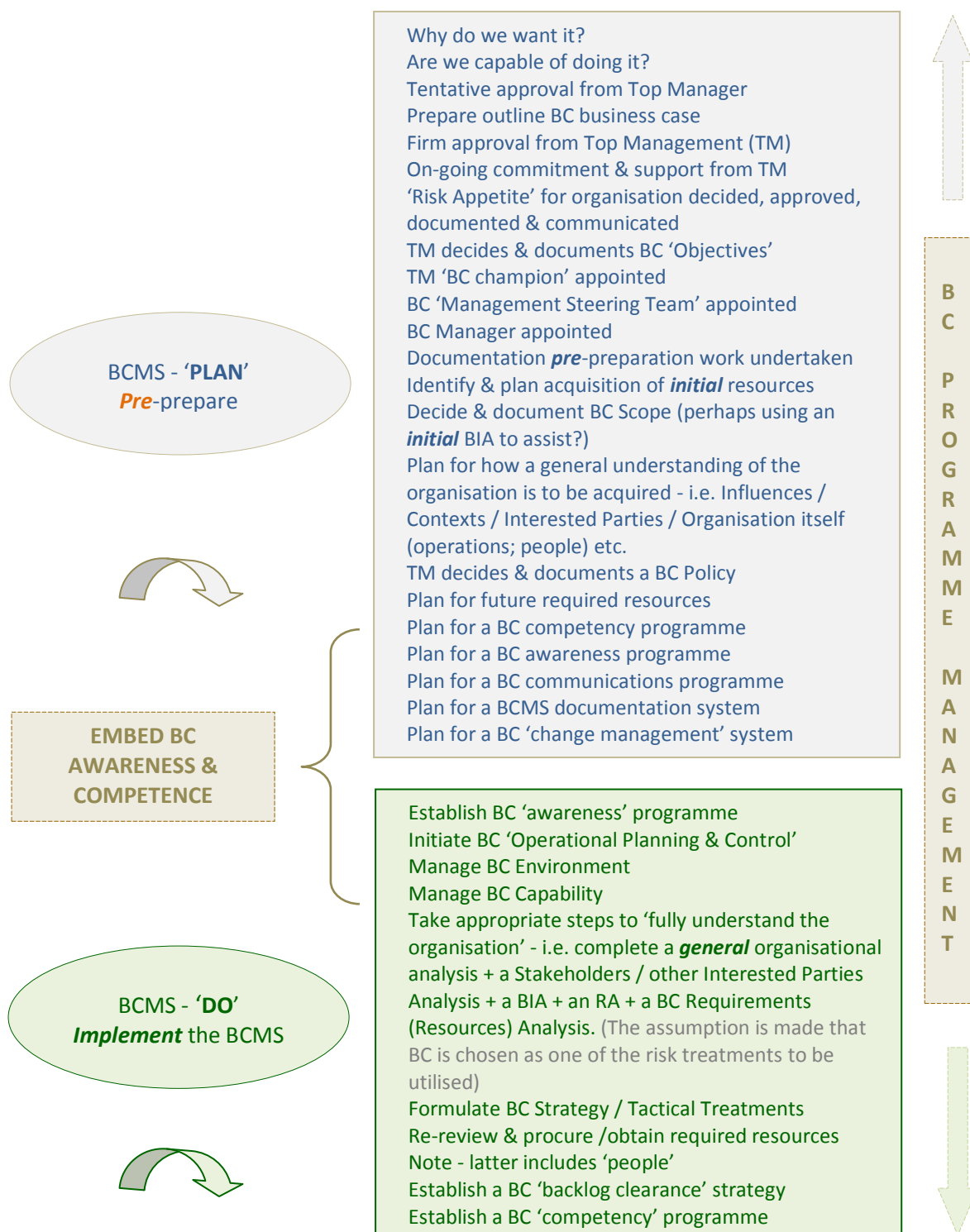
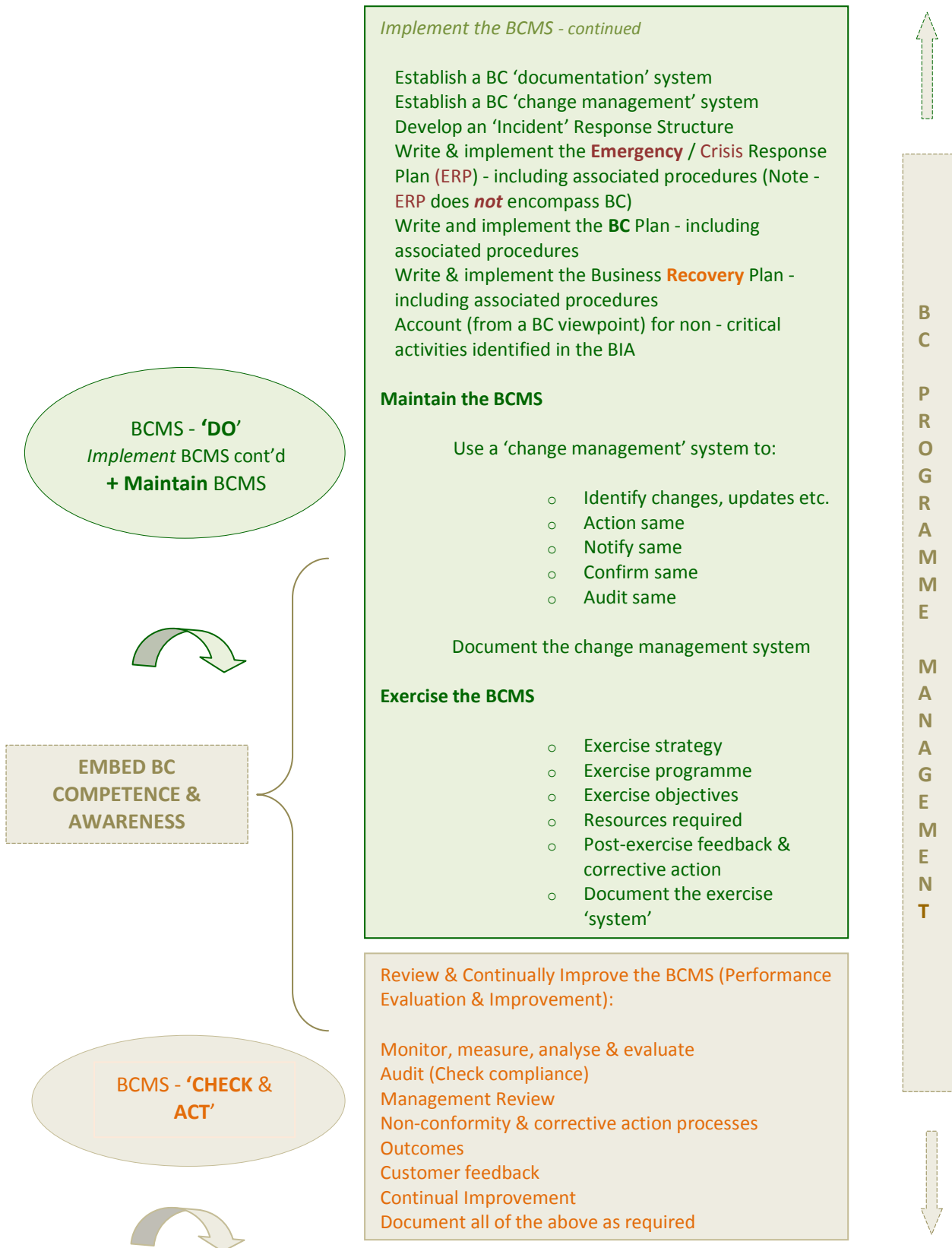


Figure 4 - Summary - PDCA's cyclical relationship with BCMS planning, implementation, maintenance and review





Figure 4 - continued





Note from Author / Owner of *this* Guideline Document

The user / reader is reminded that this guideline is very generally based on **ISO 22313** - and that the author / owner has attempted to simplify / offer further explanation of the latter (in places where it is felt that such might be of benefit to the user / reader) - mainly in an attempt to improve 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 in **ISO 22313**) - of the term '**understanding the organisation**'

As originally used in the BC standard 'BS-25999' (a major reference source [now defunct] used in the development of **ISO 22301** and **ISO 22313**), use of the term '**understanding the organisation**' was somewhat confusing and, in reality, mainly related to the conducting of two major component parts of any BC process - i.e. '**Business Impact Analysis**' (BIA) and '**Risk Management / Assessment**' (RA)

Whilst it is true that completing a **BIA** and **RA** (on an organisation) would lead to a significant understanding of **parts** of that organisation - there would certainly be additional work to do in other areas, in order 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 **scope** had included all appropriate parts of an organisation in the first place?

ISO 22313 has now arguably taken a further step backwards on this matter by not only retaining the same unhelpful use and application of the term 'understanding the organisation' as was used in BS-25999 - but has now used the same term to additionally cover a part of **ISO 22313** (not included specifically in BS-25999) related to the '**context**' of the organisation - as the following extract from **ISO 22313** indicates:

*'.....**Understanding the Organisation and its Context** (ISO 22313 / 4.1) - by determining external and internal factors which are relevant to its purpose and operations - and accounted for when establishing, implementing, maintaining and improving the organisation's 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 (page **125**)

A stand-alone explanation related to the 'context' of the organisation can be found in *this* guideline document (**sub-section 4 / 1.4** - page **86**) - under the title:

'Identify & Evaluate External & Internal BC Contexts - which are relevant to the Organisation'





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

Note 1 - section 4 / 1 refers to the necessary *pre-preparatory* steps to be considered *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 carefully that the term applies equally throughout **all** of the subsequent sections of this guideline document, but then (in such subsequent sections) **will** apply in a **different** context i.e. then being one of *continual* on-going programme management - as it applies to all elements of the **entire** BC programme management cycle

At the centre of the BC programme elements diagram (see figure 3 / page 68) is an element known as 'BC Programme Management'. This refers (in the context of this Section 4 / 1 *only* - see note 2 above) to the core management of the various, *individual projects* which require completion *before* moving on to the 'other elements'

Note - the 'other elements' just mentioned above will be covered in more depth later in this guideline

This series of pre-preparatory projects may be referred to collectively as a '*pre-preparatory programme*' - hence use of the term 'BC *programme* management' instead of the more often used term '*project* management'. However, as the programme is still actually 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:

1. Attain and retain buy-in & *on-going commitment / support* (at least in principle) for the BCMS *from* the organisation's *top management* team (ISO 22313 / 5.2 / Management Commitment)
2. *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)
3. Research and document the *requirements / reasons* (BC influences / drivers) *for introducing a BCMS* in the first place e.g. more competitive; better resilience; more profitable; regulatory reasons; other influences etc. (ISO 22313 / 4 / Context of Organisation)





4. Identify, document and evaluate 'External and Internal BC Contexts' - which are of relevance to the organisation (ISO 22313 / 4.1 / Context of Organisation)
5. Identify needs & expectations of stakeholders & other interested parties (ISO 22313 / 4.2 / Understanding Needs & Expectations of Stakeholders / [other Interested Parties])
6. Establish and document BC Objectives (ISO 22313 / 6.2 /BC Objectives)
7. Establish and document the scope of the BCMS (ISO 22313 / 4.3 /Scope)
8. Set (establish) and document BC policy (ISO 22313 / 5.3 / Policy)
9. Prepare plans for this pre-preparatory programme phase (ISO 22313 / 6.2 / Plans to achieve BC Objectives)

Note - points 1 to 9 above are expanded upon starting on the [next](#) page





4 / 1.1 - Top Management Commitment

Cross Reference - ISO 22313 / Leadership / 5.1 to 5.4

Without unconditional, demonstrable and on-going top management (TM) leadership, commitment and support of / to the planned introduction of a BCMS into an organisation - the endeavour is most unlikely to succeed. That said, it is illogical that such an endeavour would even commence without such commitment and support having already been established

The same leadership, commitment & support should apply throughout the complete programme management 'life-cycle' of an implemented BCMS (i.e. it should be ever on-going)

All *other* levels of management should similarly *demonstrate* appropriate leadership and commitment in their capacity to fulfil applicable business continuity policy, objectives etc. - in support of TM. Such 'demonstration' may be achieved using e.g. direction, delegation, involvement, motivation, engagement, empowerment, co-operation, enabling achievement and retention of associated competencies, supporting the exercise programme etc.

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

Assuming that the TM agrees with the tentative proposal, it is usual protocol for it to then be presented to the organisation's board of directors (or equivalent) for discussion, with a view to their agreement also - and assuming that this is achieved, 'work should be able to commence'

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

- Each Director (or equivalent title / grade / role / position) should *provide an outline brief to his / her own management team(s)* on the BC programme - and enlist (direct if necessary) their full commitment and support for same
- The TM should appoint an appropriate Director or equivalent (known in this guideline document *only* as the '*Top Management BC Champion*') to *provide strategic, top management oversight responsibility of the entire* (pending) *BC introduction programme* - from start to finish, and on-going thereafter - as related to the programme management 'life-cycle' of the implemented BCMS

Where necessary, an appropriately constituted '*steering / secretariat*' committee may *also be appointed* to support the 'BC champion' and to provide guidance and support to the organisation's BC Manager (see second bullet point *next* page)





Evidence / demonstration of top management (and, where appropriate, line management) commitment to appropriate aspects of the BCMS - might typically be provided by:

- Ensuring on-going compliance with relevant legal, regulatory, best practice and other appropriate requirements (ISO 22313 - 4.2.2)
- Appointing a BC subject expert(s) / specialist(s) (having appropriate authority, competency and experience) - to be responsible for the introduction / implementation of the BCMS and (thereafter) for its effective and efficient day to day operation i.e. appointing a '**BC Manager**' (5.4)

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

Note 2 - for more information see ISO 22313 - 5.4

- Overseeing establishment and effective communication (to all concerned) of appropriate * **BC Objectives & Policy** - in line with organisation's 'purpose' (6.2 / 5.3 / 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 99 and 95 respectively
- Overseeing establishment of all other (required) personnel authorities, accountabilities, competencies, experience requirements etc. - necessary to effectively and efficiently manage the implementation and on-going management of the BCMS (5.4)
- Overseeing on-going provision of adequate resources (7.1)
- Overseeing integration of BCMS processes into the organisation's established maintenance and review procedures
- Overseeing establishment and maintenance of an appropriate BCMS compliance (audit) programme (9.2)
- Overseeing / participating in BCMS management reviews (9.3)
- Overseeing & actively supporting the achievement of continual BC improvement (10.2)
- Operational involvement via steering groups, BC champion, management committees etc. (5.2)
- Active participation and support in / for training and exercising (8.5) and
- Inclusion of BCM as a permanent agenda item at scheduled top level & other appropriate management meetings (5.2)





Notes:

1. Nominated junior management and non-management representatives from appropriate (BCMS involved) departments and business units within the organisation (*required to form 'Disruption Support Units - DSUs' / see pages 107-111 for more information re this*) shall be required (where appropriate) to undertake associated roles, responsibilities and accountabilities re the pre-planning and implementation of the business continuity programme

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

DSU staff should acquire and retain the required levels of competence (training) and experience (exercising and / or involvement in real BC related incidents)

Such 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 management staff involved with the BCMS

2. Where necessary, the organisation may consider enlisting 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. For **aviation** related organisations such BC specialist(s) should be more than reasonably conversant with the appropriate aviation background of relevance (e.g. airline; airport; ground handling operator; maintenance & repair organisation etc.) i.e. **do not** engage such a specialist with e.g. experience only in banking / finance; industrial production; ICT etc.
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 / 1.2 - Documented Records relating to BC *Pre-preparatory* Programme Projects

Cross Reference - ISO 22313 / Documentation / 7.5

It will be necessary (in general) to maintain appropriately comprehensive reports, records and similar documentation - relating to most aspects of activities conducted for BC purposes (one of the main reasons being as 'evidence' of something having been done e.g. training; exercising, completion of business impact analysis etc.) This evidence is usually required for BCMS monitoring and evaluation purposes - typically related to BCMS compliance (audit) checks

It is, therefore, necessary to maintain a fit for purpose 'controlled BC document' type system within the organisation - together with robust procedures for completion, retention, safeguarding and disposal of appropriate documents - including reports and records

Note that this 'documentation system' is also 100% applicable to all BC *pre-preparatory programme projects and similar* - and should thus be complied with accordingly

Note - see [Section 4 / 6](#) of this guideline document for more on 'documentation'





4 / 1.3 - Typical Influences ('Drivers') - as related to Introduction of BCMS into an Organisation

(Note - the above title reflects how such influences [also known as 'BC Drivers'] might relate to an organisation's decision to introduce a BCMS in the first place)

Cross Reference - ISO 22313 / 'Context' / 4

Whilst many might traditionally consider brand, image and reputation as some of the most influential factors related to the potential introduction of a business continuity system into an organisation - there are other matters (internal & external to an organisation) which might be considered just as influential - if not more so

The 'figure 5' diagram (next page) presents *some* of the more common, typical BC influences (also known as BC *drivers*) - including a pictorial display indication of the comparative 'degree of influence' of each

These influences (and others) are expanded upon (in no particular order) on pages 81 to 85. Some have been provided in an aviation context

Note 1 - Fig 5 is based on * UK statistics for 2013 - (Source and © 'CMI Survey'. See article entitled 'Weathering the Storm - The 2013 Business Continuity Management Survey' - dated March 2013)

* <http://www.bsigroup.com/Documents/iso-22301/resources/Weathering-the-storm-CMI-UK-EN.pdf>

Note 2 - The 'CMI Business Continuity Management Survey of 2013' (mentioned above) would appear to have been the last published, as no further surveys are apparent for subsequent years. Thus the information regarding 'BC drivers' provided in the 2013 survey will (has) become relatively less and less useful with the passage of time

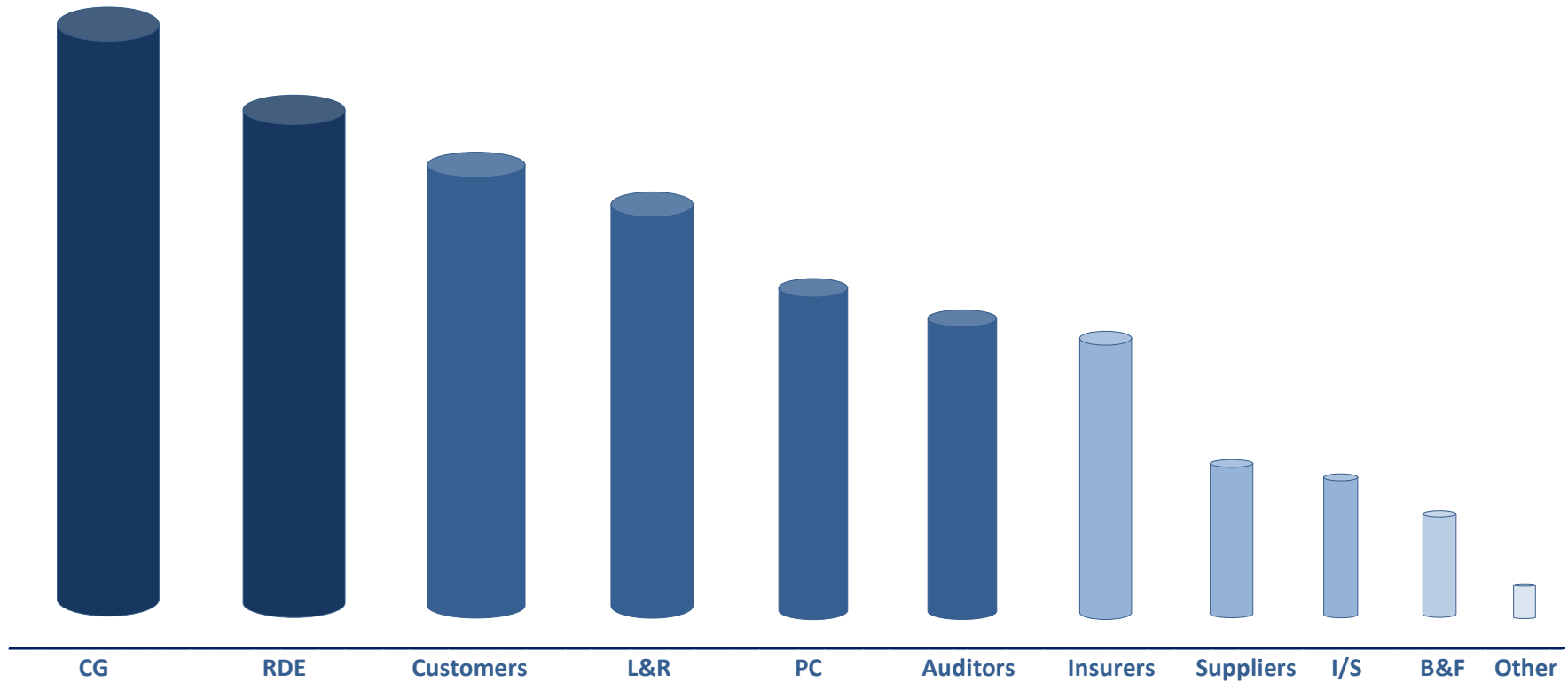
Nevertheless, it is likely that such 'drivers' will remain valid in principle for many years to come in much of the developed world. What *is* likely to change with time of course - *is the comparative degrees of influence* of such drivers

The reader should always keep this 'Note 2' in mind when studying Fig 5 - and reading pages 81 to 85





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved



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

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





More Information on BC Influences / Drivers - in no particular order

Risk - without 'risk' (or more correctly, the **threats** and associated **vulnerabilities** which give rise to risk) there would be no need for business continuity

Supply Chain - a BC issue for many organisations is reliance on key suppliers. Fuel, catering, flight despatch services, passenger and ramp services, IT / ICT and engineering support etc. - are some of the many dependencies which **airlines may** have on 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 equally to airports)

At **airports** - supply services such as catering, fuel, de-icing stocks, security, ground handling, utilities etc. - may require similar considerations

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

As a result of the above - organisations /customers (airlines and airports in the context used here) are increasingly putting pressure on their supply chains to adopt BC techniques / programmes themselves - 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. the (2012) ISO 22301 / ISO 22313 standards would be the logical choice

Note - some supply organisation standard practices can exacerbate supply chain business continuity problems - notably:

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

List Source - 'Route Map to BC Management' / 2012 - J Sharp © - The British Standards Institution 2012

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 and desirable (in appropriate circumstances) for investors to force this issue (e.g. via shareholders meetings) if an organisation is reluctant to take the 'business continuity step' 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 & reviewed





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

Similarly, 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 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 and New Year holiday period 2009 / 2010 - threatening severe disruption to tens of thousands of customers. The reason for the strike was related to actions which BA management proposed to take in order to reduce the effects of the severe financial crisis, caused by the worldwide recession at the time

BA's initial 'business continuity plan' was to take the cabin crew union to court in order to legally prevent the proposed strike. The airline won on a legal technicality and the strike abandoned at that time - 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 treatments' **should** have been *pre*-prepared by the airline

Finance / Economic / Banking etc. - although not rated highly as an influence in Fig 5 / page 80, the economic influences of the world-wide 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 essentially still pertained as at early 2018)





Political / Legislative / Regulatory **Note 1** - Legislation typically 'makes' laws. Regulation typically ensures implementation and enforcement of laws. **Note 2** - 'Political / Legislative / Regulatory' may apply at international and / or national and / or regional and / or local levels

Legal and regulatory requirement for the introduction of BC 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 documented on page 82)

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 & Local authorities (State / Regional / County / Local / City etc.)
- * 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 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 - 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 / management systems etc. are in place in order to reduce their own risk of exposure. If this evidence is not available, it is logical 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); terrorism; communicable disease (pandemic) etc.

Corporate Governance - was probably the most significant area (at least it was in the UK as at 2013 [by 2018 this had changed to 'cyber' related threats]) 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 BC introduction?)
- Adequate capabilities (including resources, knowledge & competencies) to support BC introduction?
- Prospects of top management 'buy-in'?
- Prospects of staff buy-in (including perceptions, culture, union influences etc.)?
- Potential to establish required BC 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 quickly look for a solution 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) the much more lethal 'bird (avian) flu 'goes pandemic'

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 - the above list is not exhaustive

Note 2 - the list is slanted towards the private sector (rather than the public sector). Note that the public sector has its own, unique BC accountabilities (many related to legislation and regulation) - in addition to some of those already listed above

2018 Update and Onwards

The nature of risk and its associated threats and vulnerabilities is inevitably subject to change with time

A good way to 'keep up' is to take a look at the annually produced 'Horizon Scan' - being an horizon scan of appropriate, actual and potential business / organisational risks and threats worldwide - as compiled by the UK's * 'Business Continuity Institute' (BCI) in conjunction with the UK's 'British Standards Institute' (BSI)

* Although the BCI & BSI are UK organisations, they have thousands of members all over the world - and input from same is used to compile the annual horizon scans

Please see Appendix C (page 302) of this Guideline document for more info on this matter





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

Cross Reference - ISO 22313 / More on 'Context' / 4.1

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

Ref ISO 22313, sub-section 4.1 (pages 1 & 2)

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

This subject has, to some extent, already been covered further above under the title '*4 / 1.3 - Typical BC influences*'. Where this is the case, some of these factors / issues may not necessarily be documented again here

Examples of factors / issues to account for here (where appropriate) typically include:

Evaluating Organisation's *External* Context

- 'External context' (as used here) refers to the social / cultural / political, technological, competitive, natural, criminal 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 e.g. employment, safety, communications, religion (e.g. [and referring to the latter] use of female staff in certain regimes)

How does the '*community*' *view the organisation* e.g. as beneficial, undesirable, as a threat etc.?
 - How dependent is the organisation upon *technology* e.g. ICT? 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) in which the organisation operates? Would a change of such political climate possibly change attitudes towards the organisation and its sector(s)
- What is the general *security* climate in which the organisation operates? What is the risk of *terrorism* and / or *civil unrest* affecting the organisation?
- Which *laws* and *regulations* apply and are they local, national, international?
- What *environmental* considerations does the organisation need to account 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 (closing airspace and airports), local power supply failure, disease 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* in providing the product / services / operations?
- Consideration of the results of any existing *Risk Assessments* (or similar)
 - Consideration of inter-related *external* context issues *which might have already been identified and / or evaluated by other means - including use of other 'management systems' 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.





Evaluating Organisation's *Internal* Context

Ref ISO 22313, sub-section 4.1 (page 2)

The (non-exhaustive) list below relates to the following general areas with regard to 'internal context':

- What the organisation 'does' (i.e. its key products / services / operations) - & who is / are the recipients (customers / clients) of same
- Business structure / model i.e. key main and key supporting activities required to deliver associated key products / services / operations
- Processes constituting / forming associated key main and key supporting activities
- Resource requirements associated with all of the above
- Dependencies and relationships associated with all of the above
- Organisation's operating location(s)
- Corporate governance
- Organisation's capabilities expressed in terms of available resources & knowledge
- Information (systems / types; flows etc.)
- Decision making
- Other interested parties e.g. staff awareness & commitment of / to BC concept
- Objectives and similar
- Policies and similar
- Priorities
- Potential opportunities
- Risk appetite
- Business ethics and similar
- Staff loyalty / dedication / commitment
- Internal communications
- Internal standards, best practice etc.

See ISO 22313 itself for the actual / full text





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

Cross Reference - ISO 22313 / Context / 4.2

Before starting, have a look again at the Glossary definition of '*Stakeholder (and other interested party) Analysis*' - and then relate it to what you will read below

Note - sub-clause 4.2 of ISO 22313 cannot be shown 'as written' here due copyright restrictions. However, the following provides a summary of what is documented therein. Please see ISO 22313 itself for the actual / full text:

General (4.2.1)

All organisations have stakeholders / other interested parties. Figure 6 (see page 91 of *this* guideline document i.e. the one you are reading now) provides an indication of same for the larger and / or more complex organisations

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 92)

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 which are applicable to itself and associated stakeholders / other interested parties

The information regarding such requirements should be documented and communicated internally and externally to all appropriate stakeholders / other interested parties. It should also be maintained and regularly reviewed. The review process should include emergency response planning; BC planning; risk management; hazards (e.g. storage and transport of dangerous goods) - and anything else of relevance to the organisation

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

Where appropriate, the 'international dimension' must also be considered - *and this particularly applies to aircraft operators flying international routes*





Note - After having identified (and documented) stakeholders / other interested parties as per above, you will note from ISO 22313 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:

- **Shareholders** - require a return on investment and also have an interest in the 'viability' of the organisation to continue operations
- **Customers** - require 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 - and their requirements not only need to be accounted for - but **must** also 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)

Following a major aircraft accident, survivors and the associated families, relatives and friends of all victims (alive or dead) will also expect effective and efficient communications with the airline / airport / GHA etc. involved (crisis communications) etc.

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

This can be particularly applicable to airlines (aircraft operators)



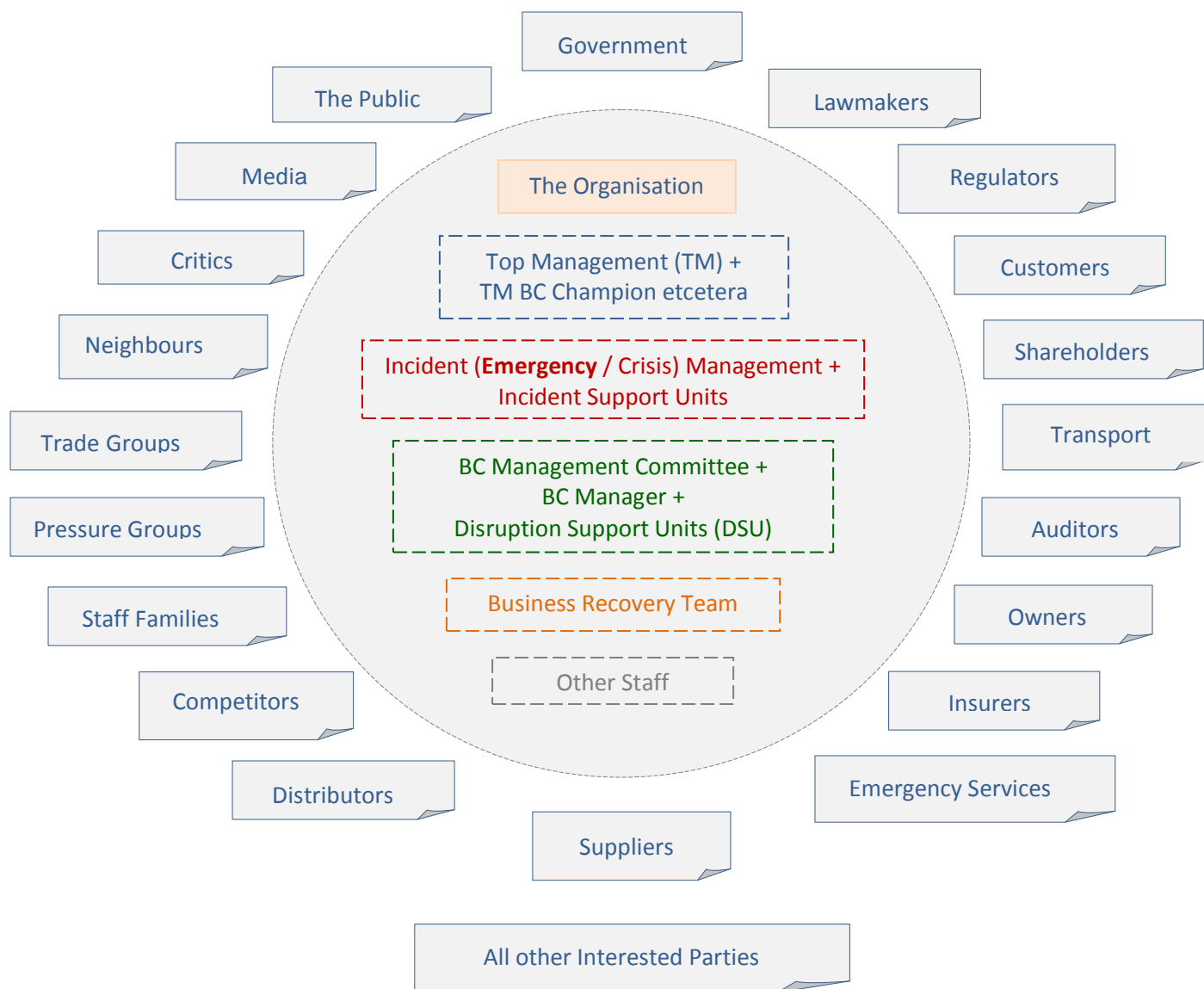


Figure 6 - The Organisation + Typical Stakeholders / other Interested Parties

Note - 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.





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

The organisation should determine how any factors, issues and / or requirements (typically as identified in sub-sections 4 / 1.3 to 4 / 1.5 of *this* guideline document i.e. the one you are now reading) will be addressed

This should involve evaluating the need for a **plan of action** to:

- prevent unintended outcomes (typically due realisation of actual / potential threats to the organisation)
- take advantage of any opportunities to improve the BCMS

.....and if necessary should also involve:

- Integrating and implementing the plan of action into the BCMS process (8.1) and
- Ensuring that appropriate & adequate **documented information** will be available - in order to **evaluate** if the plan of action has been effective (7.5)

Note - it is not particularly clear to the author / owner of *this* guideline document what **ISO 22313 / Planning / 6.1** might be referring to above. However, it probably relates to what has been referred to historically as '**preventive action**' - two **definitions** of which follow below for the information of the user / reader:

Definition 1 - Preventive Action

Action(s) taken to reduce or eliminate the probability of a specific undesirable event(s) happening **at some future time**

Preventive action is generally less costly than mitigating the effects of undesirable events **after** they have occurred, **but** may also be seen as a waste of resources if the predicted events do not take place (are not 'realised')

Risk management techniques are used to calculate the **probability** and **impact(s)** of specific undesirable negative events, in order to determine the cost-effectiveness of potential **preventive action**

Definition 2 - Preventive Action

Removing cause(s) of **potential** non-conformities / undesirable situations - by trying to prevent same **occurring** in the first place i.e. preventive action tries to prevent such **occurrence** by eliminating **cause**





Whilst ‘*corrective action*’ (see Section 6 / 2 of this guideline) aims to prevent *recurrence / re-occurrence*, *preventive action* aims to prevent *occurrence*. Both types of action are intended (in their different ways) to prevent **non-conformities**

(End of Definitions)

In general, preventive action can be thought of as a ‘*risk management / assessment*’ process

However, modern management systems had previously / historically included *preventive action* as part of their ‘*Monitoring, Measurement, Analysis and Evaluation*’ requirements - referring specifically to ‘**audit**’ (compliance) procedure - which also included ‘**corrective**’ action

As it appears that *preventive action* has now been ‘reclassified’ by ISO 22313 to be an integral part of the ‘*risk management / assessment*’ process - *preventive action* may *temporarily* be assumed (for the purposes of *this* guideline document **only**) to ‘belong’ to **both** the ‘*Risk Management / Assessment*’ portion of Section 5 / 2and also to the ‘*corrective / preventive*’ action information included in Section 6 / 2. This has been done for the avoidance of doubt

Furthermore (for the purposes of *this* guideline document **only**), the terms ‘*preventive action*’ and ‘*risk management / assessment*’ may be considered interchangeable / as having the same meaning - *when used in the appropriate context as described in the paragraph above*

The above situation will be kept under review by the author / owner of this guideline document - and the term ‘*preventive action*’ phased out in favour of the term ‘*risk management / assessment*’ - when the risk of confusion has passed

Note - ISO 22301 and ISO 22313 (both published in 2012) were the first ISO standards to conform to a new format - to which all future ISO ‘management system’ standards (new or rewrites) would similarly conform. This new format was almost certainly the reason for formally bringing ‘preventive action’ into the ‘risk management’ jurisdiction (where, in fact, it should have always really belonged)

See also Section 6 / 2 of this Guideline Document - **Corrective & Preventive Action**

See also ISO 22313 / 4.3.2, 8.2.3 & 10.1





4 / 1.7 - Establish BC Objectives + develop the Associated Plans Required to Achieve Same

Cross Reference - ISO 22313 / Planning / 6.2

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

BC Strategic Objectives

BC strategic objectives state / document the 'big picture' end purpose of what an organisation is aiming to achieve from a business continuity context i.e. they apply to the organisation's BCMS *as a whole*. In order to check (on-going) that such objectives are being *achieved*, they must be *measurable*

Top management should ensure that:

- Information relating to the setting and achieving of strategic objectives is documented and retained
- A statement is made and documented pertaining to how (in *very* general terms) the strategic objectives are expected to be achieved

Strategic BC objectives should:

- Be consistent with the organisation's BC policy (see page 99)
- Be clearly stated
- Be relevant and specific
- Be achievable i.e. both actually and within (reasonable) time limits
- Be measurable
- Be monitored, reviewed and updated - as appropriate

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





There are various methods of measuring achievement re the above e.g.

- Certification to the ISO 22301 standard is itself a measure
- Feedback from exercising (testing) is another type of measure
- If you do get the 15% reduction in insurance premium (see examples of strategic BC objectives – bottom of previous page) you *have* measured the success of the objective

For more on '*measurement*' see [Section 6 / 1](#) of this 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' (see page [99](#))

However, it is recommended that such objectives be documented separately (i.e. in their own right) within BCMS documentation for the larger and / or more complex organisations - probably positioned just before / prior to the 'BCMS Policy' section

A suggested method of identifying strategic BC objectives might be to look at your own 'wish list' of BC Outcomes (see info starting page [62](#) 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 i.e. brief, amalgamated / consolidated and to the point, as per the typical examples shown on the previous page

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

Notes:

Tactical BC objectives and associated ***plans*** are covered separately 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 shall be decided and documented separately by the organisation's '**Disruption Support Units - DSU**' themselves in their own (separate and specific) DSU BC ***plans***

(For more information re **DSUs** see pages [107](#) [starting with title 'The Workers'] to [111](#) and the appropriate sub-sections of [Section 5 / 4](#))





4 / 1.8 - Establish BCMS Scope Cross Reference - ISO 22313 / Scope / 4.3

It is important to determine and document what exactly the BCMS will and will not cover for the organisation - i.e. a BCMS **scope** is required. The scope is typically decided by the organisation itself. However, legal, regulatory, commercial and similar matters can also be influential

Scope typically applies to an organisation's:

- Key products / services / operations - plus
- Associated key main activities and key supporting activities - plus
- Any operations / activities **external** to the organisation - where desirable, permitted and possible / practicable so to do e.g. an organisations external supply chain

Scope can apply within specific timescales and / or within specific geographic locations etc.

Smaller organisations will probably wish to apply BCMS to 'everything' from the outset - whilst this might be a very ambitious and possibly undesirable approach to take 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) might serve well to direct which potential areas of the organisation should come within the BCMS scope and in what priority order - with a phased approach probably anticipated, which could possibly be spread out over a period of several years

*** Note** - whilst **formal** BIA is covered later in this document (**Section 5 / 2**), there are several good reasons for performing an **initial** (exploratory) BIA during this BCMS **pre-preparatory** phase - one of which can be used to **decide the initial scope** of the BCMS. In such circumstances, a follow-up (second / more in-depth / formal) BIA should 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 eventually form a foundation for the formal BIA

Where the above approach (initial / exploratory BIA) is not undertaken for whatever reason, then the next best method of determining the basis of the BCMS scope might be to brainstorm the matter - typically including inputs / debate from top management (where appropriate), middle management, subject matter experts (e.g. the BC Manager; external consultants), the BC champion, the BC steering group and other appropriate committees etc. External input (e.g. regulators; suppliers; subject matter experts etc.) may also be required depending on the nature of the organisation's business. Brainstorming sessions should be facilitated by the organisations BC manager / equivalent person

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 must be within every airline's scope - whereas providing restaurant type facilities for staff might be excluded

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





Some typical factors which typically dictate BCMS scope include (the list is not exhaustive):

- Types of business / output undertaken by the organisation
- Size & complexity of organisation
- Organisation's strategic objectives (note - the latter is *not* referring to 'strategic BC objectives' - but rather to an organisation's overall business objectives [*in general*])
- Needs of customers, regulators, insurers, investors etc. i.e. stakeholders & other interested parties
- Location and environment in which the organisation operates
- Resources available - particularly financial and manpower etc.

The BCMS scope should adequately account for ISO 22313 clauses **4.1** / '*Identify & Evaluate Organisations External & Internal BC Contexts*' - and **4.2** / '*Understanding the Needs & Expectations of Stakeholders & other Interested Parties*' (both also covered in *this* guideline document [the one you are now reading] in sub-sections **4 / 1.4** and **4 / 1.5** further above)

The BCMS scope is typically included within the organisation's BCMS *policy* document. The scope should be communicated to appropriate stakeholders / other interested parties

Other scope considerations include (ISO 22313 / 4.3.2):

- Ensuring that matters such as *in-scope* products, services, activities, resources, partnerships, supply chains, stakeholder / other interested parties relationships etc. are clearly distinguishable within the documented scope and, where appropriate, reflect the needs / requirements of all such stakeholders / other interested parties
- *Putting into context the scale of incident 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 process compared to **complete airport closure**)
- Identifying how the BCMS fits into the organisation's overall *risk management* policy / objectives / strategy / scope etc. - including accounting for any current / proposed *risk appetite* considerations (see also ISO 22313 / 6.1 & 8.2.3)

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 - so as to ensure that same will not adversely affect the performance and effectiveness of the BCMS





4 / 1.9 - Establish BCMS Policy

Cross Reference - ISO 22313 / LEADERSHIP / Policy - 5.3

The creation and distribution of the organisation's *BCMS Policy* statement / document, approved and signed-off by the organisation's top manager, is a key element in this *pre-preparatory* phase. It demonstrates top management commitment - in addition to providing a framework around which BCMS *strategic objectives* (related to establishment & maintenance etc. of the BCMS itself) can be set

The purpose of a BCMS policy is to document the BC principles to which the organisation aspires and against which its performance may be measured. It should also include a *high-level* overview (i.e. *not* detailed) of the organisation's BC (*strategic*) objectives and expectations

The policy also serves as an important interface between top management and the BCMS itself e.g. ISO 22301 / 5.2 requires top management to ensure that the '*BCMS is compatible with the strategic direction of the organisation*' - and a well written BCMS policy document which ticks all of the organisation's boxes regarding the subject - is one way of achieving this

The contents of a BCMS policy statement 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:

- Formulate a definition of BCMS which is appropriate to the organisation's purpose (e.g. size, nature, complexity, culture, dependencies, contexts, operating environment(s) etc.) - as expressed in terms of its overall objectives and obligations
- Identify policy components
- Identify and commit to adherence of applicable laws, regulations and similar
- Identify & refer to any 'good / best practice' guidelines available (including 'BC standards e.g. ISO 22301 / 22313') or e.g. other organisations' BCMS policy documents - which might serve as a benchmark
- *Where applicable*, conduct a * '*gap analysis*' of any current or proposed BCMS policy within the organisation - compared with the benchmarks mentioned above (and any others not so mentioned [and as available] but which might also be of benefit)
- Develop the draft of a new (or revised) BCMS policy
- Review the draft in order to ensure standardisation with other (related / appropriate) policy documents within the organisation (if applicable)
- Circulate draft policy ([internally & externally] - to appropriate parties) for consultation
- Amend the draft if necessary - to reflect consultation feedback
- Agree and implement 'sign off' of the policy with / by the top manager - and also gain approval for how the policy's is to be implemented (i.e. from a *strategic* viewpoint)
- Publish and distribute the approved BC policy document





Gap Analysis

A 'tool' used to assist an organisation to compare its *actual* performance (in a pre-defined area[s] of '*what 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 document should *include / ensure* (in no particular order):

- 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 legal, regulatory, guidelines, standards, principles, best practice, benchmarks and other policy *requirements* to be complied with or considered
- A clear commitment to all applicable requirements contained within the policy - including provision of funding and other appropriate resources
- The *resources* expected to be allocated (in very general terms)
- Details of any '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 - The top manager should appoint a Director / equivalent (known in this guideline document 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 - 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 brief overview of the roles and 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 the performance of the BCMS will be 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 management* policy / strategy





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 - an organisation's business managers are not always sensitive to low probability, high impact risks and even if they are, will probably want BC solutions geared to their own specific interests rather than to the organisation as a whole. This is where the **BC policy** comes in i.e. providing a central point of accountability for such business managers - and also 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)

See also info found at the end of the below link:

<http://www.chasecooper.com/pub-art-sub/100-business-continuity-management-1-policy-and-governance.html>

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

<https://www.lincs.police.uk/media/1648/business-continuity-management-policy-pd-90.pdf>

Lincolnshire Police Force / 2016 - This 'policy' includes the following paragraph:

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

http://www.orionjobs.com/File.ashx?path=Root/Documents/Business%20Continuity/BCF_01_Rev_3_Orion_Group_BC_Policy_2015.pdf

Orion Group / 2015

Note from Author / Owner of this guideline - 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'). If any reader / user can assist in (legally and ethically) obtaining and forwarding (to said author / owner) any appropriate, additional links re the above, they will be placed here as further examples. Please see page 10, note 10 for contact details





4 / 1.10 - Establish a BCMS conforming to the Requirements of ISO 22301

Cross Reference - ISO 22313 / Context / 4.4

This sub-section has been included here as it also appears in ISO 22313 sub-clause 4.4

The only information provided is as quoted below:

‘.....This is normative reference to ISO 22301:2012 which specifies the requirements for a BCMS. No guidance is provided’

It really says nothing more than that - and would seem to be *only* generally applicable to organisations intending to **certify their BCMS to ISO 22301**- and even then its purpose is not clear - so can it probably be ignored???





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

Deliberately Blank





Section 4 / 2 - PLAN - RESOURCING the BCMS

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

As we have seen, the *scope* of included BC related issues is typically related to the size, complexity and 'business' (what it 'does') of the organisation, and this applies equally to BC related *resourcing*. For smaller / simpler organisations, BC resource requirements are likely to be minimal - with the opposite applying to large, multi-national (and / or complex) organisations - including many airlines, airports, GHAs, MROs, Air Navigations Service Providers (ANSP) etc.

It is timely here to remember that we are still in the **Plan** phase of the PDCA cycle i.e. *pre-planning* / *pre-preparing* for how a BCMS will be introduced into an organisation. Therefore, what is now required in this **Section 4 / 2** is to identify and document all of the different types of resources needed to support such *pre-planning* & *pre-preparation*

At a later stage of this guideline document (i.e. during the '**DO**' phase of the PDCA cycle) **all** of the resources requirements going forward will * also / additionally be reviewed and then formally established / procured and allocated (ISO 22313 - 8.3.2 refers - 'Establishing Resource Requirements')

* A process included in *this* guideline document found in **Section 5 / 2** ('Business Impact Assessment - BIA') under the heading '*BC Requirements - Resources Analysis*' & also in **Section 5 / 3.5** (BC Strategy & Treatments) - under the heading '*Establishing Resource Requirements*'

It will also be recalled that at the start of a BCMS introduction programme it is vital to obtain the 'buy-in' and on-going support of the organisation's top management. This extends to approval (in principle if nothing else at this stage) for the provision of appropriate resources and associated costs / budget. Without such top-level commitment, failure is inevitable

4 / 2.1 Resources - General

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

The organisation should identify, budget for and provide / procure the resources necessary to establish and implement (and, in due course, to operate, maintain and review) the BCMS, throughout its entire life-cycle

The on-going availability of such resources - including during actual response operations to BC related incidents, should be ensured - i.e. top management should provide adequate oversight of the effective and efficient provision of appropriate resource capabilities, structures, support mechanisms and similar - which will (in all and any ways required):

- Support achievement of BC policy, objectives, strategy, operations etc.
- Be available within required timescales
- Facilitate maintenance, review and evaluation of the BCMS
- Facilitate continual improvement of the BCMS





In the process of identifying the above resources, adequate provision should be made for:

- Finance / Budget
- People type issues - including:
 - Time and effort commitments required
 - Compensation arrangements (e.g. 'time-off in lieu)
 - Establishment of awareness, competence and testing regimes
 - A system for 'managing' people (HR) related issues with regard to the BCMS
- Facilities - including appropriate work locations and supporting infrastructure e.g. equipment (including appropriate ICT hardware, software & telecommunications etc.), fixtures & fittings, utilities, washrooms, environmental, catering, alternate (backup) facilities etc.
- A 'controlled document' management system for data / information
- Associated information re the establishment of resources - including consideration of:
 - Policies
 - Stakeholders and other Interested parties
 - Legal documents (e.g. contracts, insurance policies, title deeds, etc.)
 - Terms of Reference
 - Other appropriate documents (e.g. service level agreements) etc.

4 / 2.2 Resources - Finance / Budget

From the earliest phase of any BCMS project the costs associated with acquisition and maintenance of associated resources should be estimated as accurately as possible, be approved by top management and the associated budget documented and provided

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





Some typical resources to consider for budget purposes include (NB: this list is **not** exhaustive):

- **Initial set-up costs** - especially the possibility of outsourcing BC 'expertise' (e.g. aviation related BC consultant[s]) during at least the introduction / implementation phase
- **Cost of staff** - salaries, allowances, incentive payments etc. e.g. employing a dedicated BC Manager or asking a current employee (typically Safety Manager / Quality Manager / Emergency Planning Manager etc.) to take on this 'extra' role - possibly at an increased salary?
- Costs related to acquisition, equipping and maintaining a physical '**Disruption Response Management Centre**' facility and supporting infrastructure
- Costs related to acquisition, equipping and maintaining '**alternate**' location facilities e.g. within an airline these might include alternate locations for the operations 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 Uninterrupted Power Supply (UPS) and Generators. Again, within the airline / airport etc. context, critical facilities might typically include those requiring 'alternate location' consideration - as mentioned just above
- Matters related to **Technology** continuity i.e. ICT, data, backup resources etc. (latter often confusingly and incorrectly known in the ICT context as 'Disaster Recovery')
- Matters related to **Information** (all forms / medias) & **safeguarded storage** of same
- Costs associated with staff **competency / training / exercising**
- Costs associated with on-going **monitoring, reviewing, maintaining and improving** of a BCMS - including external auditing costs (e.g. to maintain certification) etc.

4 / 2.3 Resources - People (ISO 22313 / 5.4 & 7.1.3)

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 BC Champion**' - as previously mentioned, the organisation's top manager 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'** - it is highly desirable that a small group of appropriately qualified / experienced senior managers (reporting to the 'Top Management BC Champion') be tasked with '**overall monitoring and executive troubleshooting**' of 'everything BC' within the organisation. Lower grade / rank staff with specialist knowledge can be co-opted to join this group - as required





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

- **The Specialist / Expert - 'Business Continuity Manager'** - be in no doubt that the best results for / from a BCMS will be obtained by employing a dedicated, **full-time** (sole responsibility) BC Manager - and a highly desirable requirement here is that such person should already be very familiar with **all** appropriate parts of the organisation (understanding the organisation) from the outset of the BC / BCMS introduction task. Thus an ideal candidate would be an experienced, relatively senior and longer term employee * already working for the organisation in a discipline '**related**' to BC in some meaningful way e.g. an emergency planner, a risk manager, a quality manager etc.

* As already mentioned the Business Continuity Manager should **not** 'job-share' with other roles and responsibilities if at all possible. However, it is recognised that in some (if not most) organisations, this will not be possible

Assuming that the requisite 'BC skills' (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 should **also** be appropriately familiar with the type of business [e.g. aviation related] conducted by the organisation to which the trainee belongs)

An alternative option might be to hire an **external** candidate, already qualified and experienced in BC matters. The disadvantage with this option is that for large, complex organisations the associated 'understanding the organisation' requirement can take a considerably longer period of time to achieve. Consequently, it is highly desirable (if **not 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 - in order that he / she can 'hit the ground running' - as best as possible under the circumstances

As at 2018, third party (external) Business Continuity expert consultants specialising in **aviation related BC matters** are **very** scarce - therefore, they are also likely to be expensive to engage! Nevertheless, this option may need serious consideration initially

- **The 'Workers'** - you will note later in this guideline document that (when introducing and implementing a BCMS into an organisation) there is a vital requirement to not just gain buy-in and support from the management teams - but also from the 'general workforce'. The (perhaps inappropriate) BC term historically used to describe this requirement is '**embedding BC awareness within the organisation**'. If the latter is achieved (generally not a short term or necessarily easy task) the resulting, general culture within the organisation should overall be 'pro BC'

Of course, if staff at all levels (but especially at the 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 - and this will be an important concept to relay during this '**awareness embedding**' process





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

For the purposes of this guideline document **only**, the term '**disruption support unit (DSU)**' is used for such lower level but nonetheless critical responders - **directly representing** their various parent departments / business units within the organisation

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

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

For example, during a major **airline** disruption such as closure of the major hub airport for a significant period, **DSUs** would **typically** be formed by representatives from **all** or **any** of: (Remember - we are assuming a medium to large sized airline here. The 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 in-flight catering)
- ❖ Cargo
- ❖ Commercial (including Reservations, Ecommerce and Marketing)
- ❖ 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 where so required (e.g. airline / airport 24H ops) - and in such circumstances an alternate / backup (shifts) **DSU** manning system would be necessary





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

During a major disruption all *involved* **DSUs** should have representation at a suitable and central responding and management (command, control, co-ordination & communication - [C4]) facility - which might typically be designated a '**Disruption Management Centre**' - (DMC) - which is the term used in *this* guideline document *only* (see figure 7 - page 111)

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

A back-up DMC should be planned for in case 'whatever causes the disruption' makes the primary DMC unavailable e.g. fire

All **DSU** staff should be competent 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

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

IMPORTANT NOTE - this BC guideline document (the one you are now reading) is just one of many produced by its author / owner (see page 16). Most of the others relate to how airlines, airports and GHAs plan for responding to a '**catastrophic aircraft accident**' type emergency / crisis i.e. nothing to do *directly* with Business Continuity

However, and just as aviation BC operations need manpower resources, so do emergency / crisis response operations - as per the situation referred to immediately above

The manpower 'concept of operations' *used for emergency / crisis response operations* is very similar to that described above for **DSUs** - except that the title is now '**Crisis Support Unit - CSU**' and the response is managed from a '**Crisis Management Centre - CMC**'. **CSUs** are typically formed from the same department / business unit manpower pools as **DSUs**

For airlines in particular, a worst case scenario for emergency / crisis response should 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 the 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 and total shutdown for the associated airport

In this worst case (but nonetheless realistic) scenario the accident *airline* is deploying its **CSUs** and *eventually* its **DSUs** concurrently - managing both respectively from the (separate facilities) **CMC** and the **DMC**. The scenario further assumes that the airline is also trying to conduct concurrent '**normal**' operations across its network - other than those at the accident airport itself





What all of the above means in reality is that when considering the manpower resources required for worst case emergency / crisis type scenarios - **airlines** must **additionally** plan to provide (separate) manpower resources for **eventual BC operations** - and to also account for **ongoing 'normal' operations**

It is not 'rocket science' to see that this will cause major manpower resource problems for any airline. Nevertheless, this will be the situation 'on the ground, on the day' - and it must still be **managed (and pre-planned for)** - and appropriate solutions found (even if they are 'workaround' type solutions)

Using the same worst case scenario as per above - the accident **airport** is typically somewhat better off than the airline - as it (**the airport**) needs to conduct just (only) emergency / crisis response operations until such time as it re-opens for business. Whilst preparations for **airport** re-opening will obviously be required (e.g. removing accident aircraft; recovering and removing human remains and personal effects; repairing damage to airport infrastructure) - this will not necessarily require activation of the **airport's** BC response

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

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 will also need to concurrently respond to their **own** continuity disruptions and normal ops demands

Lastly, whilst this 'important note' relates to **manpower** resources, other types of resources may be similarly impacted by the need to provide two contingency responses concurrently (emergency / crisis response operations & BC operations) whilst also maintaining concurrent normal operations e.g. it would border on recklessness to 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 be planned for**



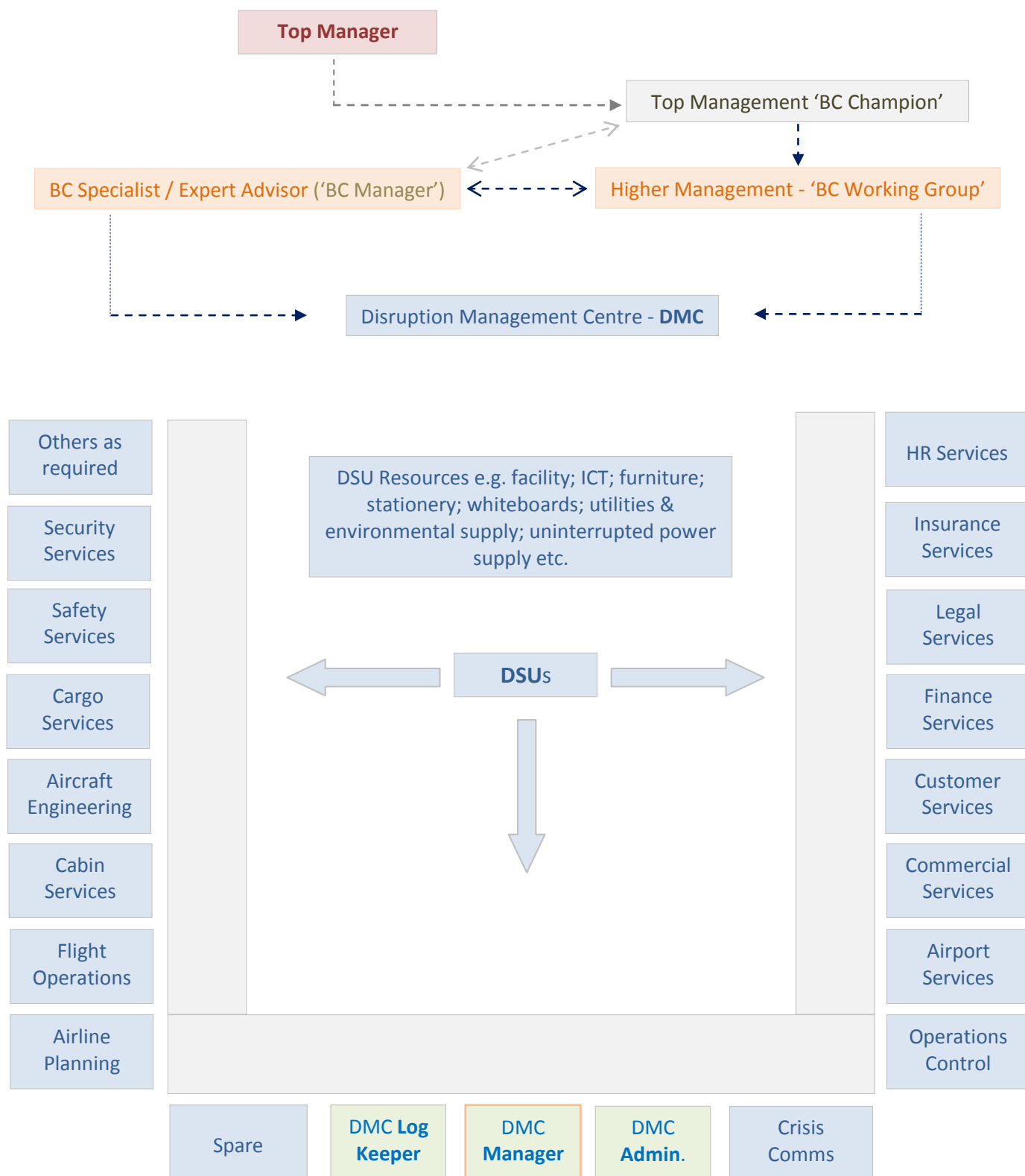


Figure 7 - Typical Airline DSU Layout





4 / 2.4 - Resources - **Infrastructure, Facilities, Equipment, Technology, Information** etc.

The above resources and similar have already been referred to in the General (4 / 2.1) and Finance / Budget (4 / 2.2) sections further above

4 / 2.5 - Resources - **Documentation**

The 'BC Resources Programme' should be appropriately documented. See *Sub-section 4 / 6* of *this* guideline document for more information

For cross reference purposes the subject of *BC resources* also appears in:

Section 4 / 1 / 1 of this guideline - based on:

ISO 22313 / 5.2.f) - **LEADERSHIP** / Management Commitment

Section 4 / 2 of this guideline - based on:

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

Section 5 / 2 of this guideline - based on:

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

Section 5 / 3.5 of this guideline - based on:

ISO 22313 / **OPERATIONS** / BC Strategy - Establishing Resource Requirements - 8.3.2

Note - there is a significant degree of overlap in the ISO 22313 sourced clauses above. Little effort seems to have been made within ISO 22313 to better manage / mitigate such overlaps (which may be potential source of confusion to some users / readers)





Section 4 / 3 - PLAN - EMBEDDING AWARENESS

Cross Reference - ISO 22313 - 7.3 'SUPPORT / Awareness'

The term 'embedding awareness' is a relatively confusing way of saying that just about everyone in an organisation, top to bottom, should be:

- Reasonably aware of BC related matters, in general, within the organisation
- Aware of any personal BC roles, responsibilities and accountabilities (and, having become so aware, will naturally [hopefully] wish to support the concept and application of BC within the organisation)

The concept of 'embedding BC awareness in the organisation' is good in principle - but can be difficult to achieve in reality. Some reasons for this are:

- Some personnel, already overworked with regard to their *primary* duties within the organisation, will now be asked to take on additional BC responsibilities (probably / usually without reward or compensation). They will typically be 'asked' to do this because they are probably the only people within the organisation capable of 'doing what is required' (e.g. an organisation's safety manager / emergency planning manager [single person with **dual** accountabilities] - now also being assigned BC accountabilities [i.e. assigned a **third** accountability])
- BC responsibilities generally only 'drill down' as far as those involved at **Disruption Support Unit** level, leaving many staff outside of the 'BC loop' - no matter how much the subject is 'advertised / promoted' within the organisation - i.e. BC awareness programmes, no matter how promulgated and applied within an organisation, will probably be of little or no interest to some staff - and thus will be ignored, if it is 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 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 contentious where blame might be attributable

On the plus side, we have already seen some of the benefits of running a BCMS programme within an organisation (see page 61) - a number of which will be directly beneficial 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 & difficult process of 'embedding BC awareness' - will be well worth persevering with and, if implemented sensitively, logically and fairly - will probably enhance (even if only in the longer term) the experience of working within the organisation

We have mentioned earlier in this guideline document the concept of '*understanding the organisation*' and such understanding is vital in working out the best way to embed BC awareness

Awareness is obviously achieved directly (e.g. by training & exercising) by those having formal BC roles & responsibilities. Additionally, various other methods may be employed to raise awareness amongst all staff (with formal BC roles or otherwise) including:

- Suitable commitment in organisation's Mission Statement, BC Policy document etc.
- Workshops
- Information documentation (flyers, short information brochures etc.)
- Regular awareness programme via the organisation's internal communications setup (e.g. via email; via websites / intranet; via simple eLearning systems etc.)
- New staff induction programmes
- Inclusion of BC as an ongoing topic in team meetings
- BC participation linked to pay and promotion prospects for certain personnel
- Publicising 'rewards and / or recognition' 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 internal publicity related to BC exercise planning and feedback and the actual exercises themselves to reach out to as wide an audience as possible - even to those not directly involved with such exercises

In particular, high profile BC awareness campaigns should be run before and during the *initial* introduction and implementation phases of BC to an organisation, so as to try to ensure that everyone understands the associated reasons and benefits. Following this, further campaigns might be run once the actual BC plans and supporting infrastructure become operational

It is particularly important to win over *middle management* staff as many are very experienced and understand the organisation reasonably well (at least in parts) - and accordingly will almost certainly be drawn in (in some way or another) to BC activities, voluntarily or otherwise

'Voluntarily' is obviously the preferred method and extra care should be taken with this latter group in efforts to get them to become 'pro-BC' - rather than simply trying to impose it (the latter will generally not work - at least not to the desired outcomes!)





It is also particularly important to win over those involved with procurement and logistics i.e. those dealing with suppliers, outsourcers, intermediaries etc. If these personnel are pro-BC it is likely that they will try to ensure similar applies with their suppliers etc.

Lastly, it will be necessary to also increase awareness of the organisation's commitment to BC - 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 61)

The above just about 'wraps-up' the subject of 'embedding awareness'. However, the user / reader should also take a look at what the standard says:

ISO 22313 (page 10) / SUPPORT / Awareness - 7.3





Section 4 / 4 - PLAN - EMBEDDING *COMPETENCE*

Cross Reference - ISO 22313 - 7.2 'SUPPORT / *Competence*'

All BC designated responders within an organisation, at all levels, need to be competent in what it is that they will be doing during actual BC operations i.e. as related to specific roles / responsibilities - and also in acquiring a general concept of the organisation's overall BCMS and their place in it. This is typically achieved via a regime of initial and recurrent training and frequent exercising

Those (small number of staff) responsible for managing BC 'command, control, co-ordination and communication' (C4) operations need to *additionally* acquire the knowledge level status of '*expert*' in all aspects of the organisation's BCMS - both theoretical and practical

The training resources can come from within the organisation itself e.g. via the BC Manager conducting the training and exercising programme; via eLearning etc.

It is highly desirable that a BC '*train the trainer*' programme is also initiated - drilling down to *Disruption Support Unit* level - in order that such units are eventually capable of conducting their *own*, specific internal BC training and conducting their own (*DSU* specific) modular BC exercises

Training resources can be outsourced (i.e. 'instead of' or 'in addition to' internal training). However, a major disadvantage here is that there will typically be a lack of 'understanding the organisation' compared to the in-house option - and, as previously mentioned, there are very few BC experts (trainers) capable of adequately delivering such training in an *aviation* related context

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, town and county councils) and regional health authorities etc. are legally required to have both BC plans in place and to conduct associated BC training. This is mandated by the UK's 'Civil Contingencies Act (Law) 2004'

As mentioned earlier, the above also applies to UK *airports* BUT, paradoxically, not to UK *airlines*!

The following 'competence development programme' should be planned for & implemented:

- Identify, define & document required BC competencies
- Identify and document training requirements - as associated with BC competencies
- Produce the associated 'textbooks' (training notes)
- Procure and establish the required training support resources
- Identify, engage and establish / prepare the trainers
- Decide *who* (which target groups) receives *what* training (e.g. 'initial', 'advanced', 'recurrent', 'train the trainer' etc.) - *when* (e.g. six monthly; annually) - to *what levels* (e.g. basic, intermediate, advanced, expert etc.) - and *how* (e.g. classroom; self-study; CBT / E-learning etc.)





- Deliver appropriate types of training to target groups - at designated frequencies
- Monitor & measure training delivered versus attainment & retention of required competencies
- Establish, maintain and improve BC skills / experience competence - by establishing a regular and specifically targeted BC '*exercise*' regime
- Maintain the competence development programme
- Regularly review the competence development programme
- Strive to continually improve the competence development programme
- Control and maintain associated documentation (reports and records etc.)

Note that personnel from external parties (engaged by the organisation on longer term projects) should be contractually required to attain and retain an appropriate level of BC competence (should the latter be necessary) - as related to the work for which they have been engaged

The organisation should also make every effort to ensure (insofar as is permitted / practicable and desired) that external parties involved in the 'supply chain' to the organisation (regarding 'supplies' categorised as 'critical' to the continuity of the organisation's product / services / operations) also achieve and maintain associated and appropriate 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) leading, in turn, to the issue of formal BC terms of reference and / or BC role / job / task descriptions - against which performance can be monitored and measured

The above just about 'wraps-up' the subject of 'embedding competence'. However, the user / reader should also take a look at what the standard says on the subject:

ISO 22313 (page 8) / SUPPORT / Competence - 7.2





Section 4 / 5 - PLAN - COMMUNICATIONS

Cross Reference - ISO 22313 - 7.4 'SUPPORT / **Communication**'

For related matters - see also ISO 22313 - 8.4.3 and 8.4.4.3.2

Communications with Stakeholders / other Interested Parties

See also the '**DO**' Section of this guideline - 5 / 3.8 (page 225) - for additional guidance

Effective, efficient, co-ordinated and consistent communications are an essential component of any contingency response - including business continuity operations. The following should be considered (and addressed where appropriate) when planning for and setting up same:

- The BC 'communication' needs of all 'stakeholders / other interested parties' (internal and external to the organisation) should be adequately accounted for. This includes communications utilised during any 'BC Awareness' type activities
- All methods of BC communication appropriate to the organisation should be utilised e.g. written (hard copy; soft copy); spoken (training, briefings etc.); via appropriate website(s) and social media etc.
- Appropriate resources should be procured / established and regularly maintained / tested - such resources being necessary to adequately implement the requirements of the primary methods of BC communications planned for
- Back-up (alternative) means of BC communicating should be procured / established and regularly maintained / tested
- The communication needs of the organisations 'BC alerting / activation system' should be particularly accounted for - and even more particularly those which are ICT related
- Appropriate staff (e.g. Top Manager & deputy; DMC Managers; the **Corporate Communications / PR** Disruption Support Unit [DSU]) etc.) should be required to achieve an appropriate level of competence in BC communications – particularly media related crisis communications
- The ability 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
- A documented system should be established to manage and record all appropriate forms of BC related communication sent / received. This should include a comprehensive, current and accurate database of all contact information considered necessary to manage and operate an adequate BC response
- Operating and testing (exercising) of the organisation's BC communications capabilities





Section 4 / 6 - PLAN - DOCUMENTED INFORMATION

Cross Reference - ISO 22313 - 7.5 'SUPPORT / Documented Information'

Purpose of Establishing, Maintaining and Retaining BC Related Documented Information

To provide clear evidence of the effective preparation, implementation, operation, maintenance and review of an organisation's BCMS i.e. to provide evidence of conformity to BCMS requirements and effective, efficient & expedient BC operations

General

If an organisation is intending to prepare and formally **certify** its BCMS in compliance with the **requirements** of **ISO 22301**, certain specified documentation *** must** (i.e. compulsory) be established, maintained and retained. You will find the associated list in **ISO 22313** (7.5.1 - General [page 12])

* Note - formal certification requirements also specify that certain *additional* documentation **may** (i.e. **advisory**) also need to be established, maintained and retained. You will find the list of additional documents as per the reference already given above

If an organisation is intending **instead** to prepare and formally **align** its BCMS with the **guidelines** contained in **ISO 22313** - then it is obviously a very good idea to also follow the documentation requirements listed in the paragraph immediately above

If an organisation simply wishes to use **ISO 22313** to **guide** its BCMS preparations in general, it is recommended that the guidance re documentation provided in (ISO 22313 - 7.5.1 - General [page 12]) is still followed - insofar as is deemed compatible with the size, complexity and nature of business of the organisation concerned

Control of Documented Information

The greater majority of airlines, airports, ground handling agents etc. should already be familiar with the requirements and operation of a '**controlled document system**' - as an integral part of 'what they do' during normal operations

As such, this subject has consequently been excluded from the scope of this guideline (except to state that without such a system in place [managed by appropriately competent people] and supported by an appropriate document management system [manual and / or via an appropriate IT tool] - the task of planning, implementing and managing BCMS will probably be **** unnecessarily cumbersome and subject to error**)

**** Except (possibly) for the smallest / simplest of organisations**





Confidential, Personal, Proprietary & Similarly 'Protected' Documentation

Proper care should be taken to ensure the appropriate protection (safeguarding) and non-disclosure of confidential and similar documented information (including 'personal' information)

The organisation should comply fully with all relevant legislation and regulation (including appropriate 'data protection / personal privacy' and similar issues) regarding the retention of documented information - and establish, implement and maintain the associated processes required to achieve compliance





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 and are now ready to start '**doing**' (i.e. the 'implementing & operating' part of the PDCA cycle)





Deliberately Blank





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 and control** its BCMS needs and requirements, as outlined in [Section 4](#) of this guideline i.e. the various **elements** of the required business continuity programme management project (see again pages [65-71](#)) must now be actually established (put in place) and managed

The 'control' referred to above typically includes:

- Invocation (establishing) of the implementation plan and associated methodology - which should have already been pre-prepared as per [Section 4](#) of this guideline
- 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)
- Operating an appropriate 'change management' system
- Maintaining an associated 'documentation management and information' system

Elements of Business Continuity Programme Management - BCPM

As a reminder, the elements of BCPM comprise (refer to the Glossary where required):

- 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 appropriate 'BC Tactical 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!' e.g. write the associated BC and business recovery plans; set-up an appropriate 'incident response structure' - including acquisition of associated resources (particularly manpower); establish required degrees of competency (training) and experience (exercising + actual BC operations [if any for latter]) etc. - all covered later in this [Section 5](#) [cross-reference ISO 22313 - 8.4 & 8.5])

Note - ISO 22313 rather confusingly entitles the requirements of the paragraph immediately above as '*Establish & Implement Business Continuity Procedures*'! (The confusion coming from use of the word '**procedures**')





The initial establishment and ongoing management etc. of the BCPM should be assigned to the designated personnel resources already identified in Section 4 of this guideline

Note that ISO 22313 includes a further 4 sub-sub-clauses under sub-clause 8.1.

- Managing the BCMS environment (8.1.2)
- Managing BCMS capabilities (8.1.3)
- Measuring BCMS effectiveness (8.1.4)
- BCMS Outcomes (8.1.5)

Just about everything covered in these 4 sub-sub-clauses has been (or will be) covered in this guideline (i.e. the document you are reading now) - and is also expanded upon in greater detail in other parts of ISO 22313 itself. Nevertheless, it is recommended that the user / reader takes a look at the original ISO 22313 text

Reminder - when using this guideline document you should also have ready access to the **ISO 22313** standard (document) 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 might be advisable for the user / reader to re-review the appropriate Glossary terms:

- ✓ Activities
- ✓ Business Impact Analysis
- ✓ BC Strategy
- ✓ BC (Tactical) Treatments
- ✓ Business Continuity Requirements - Resources Analysis
- ✓ Critically time-sensitive processes / activities + associated resources & dependencies
- ✓ Key Product / Service / Operation
- ✓ Maximum Tolerable Period of Disruption (MTPD)/Maximum Acceptable Outage (MAO)
- ✓ Minimum Business Continuity Objective (MBCO)
- ✓ Process
- ✓ Recovery Time Objective (RTO)
- ✓ Risk
- ✓ Risk Appetite
- ✓ Risk Categories
- ✓ Risk Management (including Risk Assessment)
- ✓ Risk Treatments
- ✓ Stakeholder (+ Other Interested Parties) Analysis

Also consider reviewing 'Preamble Note 6' - starts page [7](#) of this guideline document

Also consider reviewing 'BC at its Simplest' - starts page [53](#)

Also consider reviewing the 'Note' (Understanding the Organisation) - page [72](#)

Also consider reviewing Section 4 / 1.5 - (Understanding the Needs & Expectations of Stakeholders / other Interested Parties) - starts page [89](#)

Also consider reviewing Section 4 / 1.6 - (Actions to Address Risks & Opportunities) - starts page [93](#)

*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*





Understanding the Organisation

Introduction

An organisation achieves its 'purpose' by delivering its key products / services / operations / whatever - to customers (whoever or whatever the customer might be). Consequently, it is important for the organisation to clearly **understand** the adverse impacts (over time) that **disruption / interruption** of such key products etc. (together with their associated [supporting / subordinate] **key activities**) might have on its business, and thus on its customers

It is important to **understand, in turn**, the associated inter-relationships / inter-dependencies and resource requirements of the **supporting / subordinate** key activities mentioned above

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 / treat'** (or possibly take advantage of) the impacts of same. This process is known as 'risk management'. One (but only one of several) such risk 'counter / control / treatment' is to apply BC measures - if the circumstances are appropriate so to do

Note - In order to adequately achieve the above 'understanding' requirements, an organisation needs to clearly identify its key products / services / operations from the outset of the 'understanding the organisation' task

Reminder - very generally speaking there are 5 'methods' of 'dealing' with threat related risk. Four of them are applied **before** the risk actually occurs in order to prevent the risk 'realising' (actually occurring). The fifth is deployed to manage the risk **after** it has actually occurred - otherwise known as **business continuity planning** (See figure 19 - page 182)

Apart from its use within the BC context only, **Risk Management as a subject lies outside the scope** of this guideline

Taking all of the above together, an organisation can identify and analyse such potentially disruptive impacts and their consequences (we shall see later in this **Sub-section 5 / 2** how this is achieved) in order to come up with a high level action plan (known as **BC Strategy**) for how (going forward) such consequences might be dealt with - **from a business continuity context**

More specifically and practically, **the person(s) primarily responsible within the organisation** for introducing, implementing & maintaining a BCMS must acquire, retain, monitor, review and document the 'understandings' referred to further above - together with ascertaining how any associated threats might be dealt with (*** in the BC context only**) by application of appropriate BC measures (known as **'BC Tactical Treatments / Controls'**) - which meet the requirements of an associated **BC Strategy**

* Such threats obviously **also** need 'dealing with' outside of the BC context i.e. within the **Risk Management** context. As already mentioned, this latter subject falls outside the scope of this guideline





Of course, the *scope* of the degree of understanding required is linked directly to the scope of the BCMS as included 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 to implement a BCMS, then the breadth and depth of understanding required will be far different from 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 or accomplished ineffectively, then the associated BCMS will simply not deliver what is required e.g.

- Threats & associated vulnerabilities (risks) to the continuity of operations might remain 'undiscovered' and thus not be accounted for
- Appropriate and / or adequate BC strategy / tactics / plans might not be available
- Appropriate and / or adequate (non-human) resources might not be available
- Appropriate and / or adequate BC responders / teams might not be available and - even if available might not be available in time - and even if available in time, might not be competent to carry out required BC roles, responsibilities, assignment 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 the organisation'?

1. *By involving the Most Appropriate Personnel*

The Theory

In theory, perhaps the best way to gain an overall and reasonably rapid 'understanding of an organisation' is to assign / second appropriately skilled / experienced, *middle level* management staff to key BC positions, right from the start of the BCMS programme (there would also be other advantages in doing this of course)

Such managers (if chosen with care) should typically *already* have a reasonably good understanding of how the organisation functions in general, as a result of 'what they do' within the organisation. For example, in the aviation context, such staff might typically have backgrounds, knowledge and experience in e.g. Risk Management, Quality Management, Emergency / Crisis Response Management, Safety Management and possibly Insurance

The above managers might be supported in their BC roles and responsibilities by a seconded team of 'subject matter experts' - drawn from those departments / business units which are expected to be assigned roles, responsibilities and accountabilities under the BCMS





All of the above staff should be provided with the required degree of BC competence & basic experience (e.g. via training & exercising - one or both possibly acquired externally) - together with the appropriate 'business tools', resources and support to do the job

The Reality

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, (in reality) it is more than likely that the BC Manager will be sharing his / her BC accountability 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 bottom of the previous page) and then further 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 the change might be - including the introduction and implementation of a BCMS. 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 might 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) can be overcome - thus permitting the desired, valuable and continuing contribution of such staff

The BC Manager - BCM (or equivalent title) - looked at from an aviation related context

If no BCM position(s) or equivalent (e.g. an airline's / airport's Quality or Safety Manager also 'doubling-up' as the BC Manager) currently 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 - and an approved budget)

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 external, **aviation specialist** BC consultant might be engaged to undertake the 'understanding the organisation' task - with the 'permanent' (designate) BC Manager 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 - no doubt at some financial cost. However, this might be a viable option provided (again) that the organisation's permanent BC Manager designate be required to 'learn on the job' - e.g. by understudying said consultant throughout the project

IMPORTANT - The use of a non-aviation specialist BC consultant(s) is best avoided - for 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 relatively few of them in the world

2. By Use of appropriate 'Business Tools'

When undertaking the 'understanding the organisation' task it has become standard practice to use certain 'business tools'. The main tools used are:

- **Stakeholder** (+ other Interested persons) **Analysis**
- **Business Impact Analysis** (BIA)
- **Risk Management** (Analysis / Assessment) (RA)
- **BC Requirements - Resources Analysis**

Some overview notes on these tools start immediately below. More detailed information on the application of Business Impact Analysis and Risk Assessment is shown in [Section 5 / 2B](#)

Stakeholder / other Interested Party Analysis - see also [Section 4 / 1.5](#) of this guideline

This analysis is a useful starting point in 'understanding the organisation'. At its simplest, it typically requires a brainstorming session(s) with appropriate parties (probably the middle level managers & subject matter experts as already discussed further above on page 127) - to identify all (other) possible 'stakeholders / other interested parties' associated with the organisation from the BC context. They are then placed in an initial, listed *order of importance* (related to what they *expect* from the organisation and *vice versa* - such *expectations* also being listed alongside the associated stakeholder / interested party)

This initial list is then used to assess the adverse impacts of significant (uncontrolled / non-specific) disruption on the organisation in general - *as related to the listed expectations* and, if necessary, the order of importance (of the latter) on the initial 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. etc.

Whilst 'customers' will typically rate highly on the '*importance*' list - there will usually be little choice other than to place legal and / or regulatory and / or similar interests at or near the top





Appropriate suppliers may also rate highly e.g. if it eventuates that defined aspects of an organisation's business continuity operation will depend, in turn, on those of an identified supplier / suppliers - then the organisation also needs to account (in whatever way is most appropriate to circumstances) for the business continuity capabilities and requirements of such supplier / suppliers

The importance of the media should not be discounted here as they can and do exert a very significant influence on the 'public'. Any airline / airport etc. mishandling a 'major disruption to business' event can expect a hard time from TV, newspapers, electronic (social) media etc. - including consequent, adverse impact on brand, image and reputation

Also note that pressure groups can (and have) 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)

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 of operation) *the organisation's key products / services / operations* (together with associated key main and key supporting activities and their 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 pages 155 to 162) should be 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](#)

General

BIA (when taken together with the other three components [business tools] of the 'understanding the organisation' process [see previous page]) may be regarded as the foundation of the Business Continuity Programme Management. In brief summary it (BIA) is all about:

- Identifying an organisation's *key product(s) / services / operations*
- * 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





- * Assessing the **impact** of (uncontrolled & non-specific) disruption / interruption on each identified **key main activity** - as related to delivery of the **associated key products / services / operations**

'Score' each result in 'units' of impact assessment (for **eventual** input into the risk management (assessment) matrix [see examples in figures 11 to 17, pages 163 to 171]) and in terms of 'priority for action' (e.g. 'highest', 'high', 'medium', 'low' and 'for possible future attention')and (+)

- * Assessing the **impact** of (uncontrolled & non-specific) disruption / interruption on each identified **key supporting activity** - as related to delivery of the **associated key main activities**

'Score' each result in 'units' of impact assessment (for **eventual** input into the risk management (assessment) matrix [see examples in figures 11 to 17, pages 163 to 171]) and in terms of 'priority for action' (e.g. 'highest', 'high', 'medium', 'low' and 'for possible future attention')and (+)

* **Reminder** - from the glossary meaning of the term 'activity' as used above and elsewhere in this guideline, most (if not all) activities are typically made up of a series of associated **processes**. For the sake of simplicity and brevity the latter are ignored

However, when conducting a BIA in reality, all such processes (as associated with each key **main** activity and key **supporting** activity) **must** also be accounted for - and be assigned MTPDs, RTOs and MBCOs (see Glossary) **in their own right** where appropriate (in the same manner as already described above) - and the results documented accordingly

Furthermore, it will also be necessary to include in the BIA (with regard to associated key activities of whatever type) staff; systems, equipment, documents & records; facilities etc.

- Estimating & applying associated **MTPDs** based on the results of the above - as appropriateand (+)
- Estimating & applying MTPD associated (initial) **RTOs** based on the results of the above - as appropriateand (+)
- 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 above) to adequately account for sameand (+)





- Setting the minimum level of operation (**MBCO**) to be achieved when a disrupted activity is assumed to 'resume' at the RTOand (+)
- Identifying '**single points of failure**'and (+)
- Using **impact** level assessments (scores) from above as **inputs** to the **associated risk management** (assessment) processand (+)
- **Pulling together & documenting** the results of all of the above into a report which, (when combined with the results the other three components [business tools] of the 'understanding the organisation' process and approved by top management) will be used in due course to formulate a **BC Strategy**and (+)
 - **** The **BC Strategy**, in turn, outlines [from the higher level BC viewpoint] what the organisation needs to achieve going forward from the BIA - in order to try to ensure continuity of its key activities (in the BC context only), following a significant disruption event to same e.g. formulation of 'BC Tactical Treatments', setting up of the '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. 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**

***** IMPORTANT NOTE** - a BIA typically works on a worst case scenario, typically based on the concept that the impact of a significant disruption event on a particular activity - leads to the **complete cessation** of such activity

However, 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

The BIA can sometimes be a difficult task to perform competently but is one of the most critical to get 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 and analysis of same





Seasonal / Calendar Variations

Within the BC context a **further application of time** must also be considered i.e. certain key activities become more time-sensitively critical (more urgent and / or of higher importance) at certain times of the year e.g.

- Aircraft and crew enhanced availability 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 operations) 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 should generally be made that 'disruption' 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) e.g. a single person (in a small airline) maintaining the entire on-board aircraft documentation required to conduct public transport flight operations; e.g. an airline using a single in-flight catering supplier at its main / hub base (with no alternate supplier provided for); e.g. an airport using just one type of navigational guidance aid to its main runway(s); e.g. an airline / airport / GHA etc. using a digital telephone system with no analogue telephone system backup; e.g. ICT servers having no off-site backup capability etc.

Scope of the BIA

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, 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 pre-planning 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





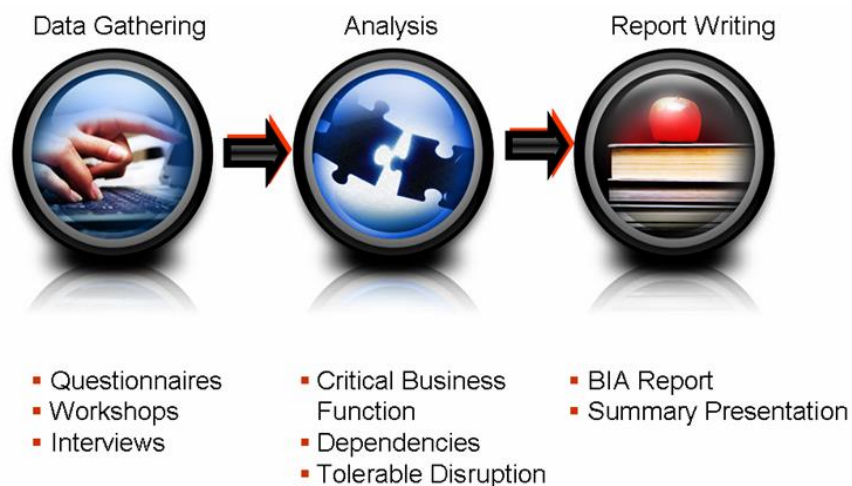
BIA derived data / information can also be used retrospectively e.g. to possibly revise previously decided matters (e.g. the *initial* BCMS *scope* and *initial* estimates of *resources* required - as documented in the organisation's 'first try' BC Policy document) for which appropriate BIA derived material might not have been available at that 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 [management] assessment) will directly influence which *BC Strategies* (and thus, in turn, which associated *BC 'Tactical Treatments'*) are finally chosen for implementation - and will also be used to assist in the 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](#) and [Section 5 / 4](#) for more information concerning the above

The BIA process might be summarised (*very* simplistically) as follows:



See [Section 5 / 2B](#) for more detailed information on the BIA process itself



Note - the process of ranking / grading / scoring (i.e. prioritising for remedial action) **time-sensitive** activities - may be explained as:

*'A priority ranking system for an organisation's key main and key supporting activities (as appropriate), the loss of which is * usually (but not always) proportional in terms 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 etc.

As an example of what this means in practice - take two important airline activities - such as operating the main (only) 'call / contact / information / reservations centre' - and the provision of 'in-flight catering' for its flights - and assume that both activities are seriously and simultaneously disrupted by a 'crisis' event (whatever that crisis event might be) - and that 'time' to recover is a factor (which it really is of course - for both activities)

Without a call centre, no calls can be received - thus no (or much reduced) business gets done - thus adverse customer service and financial etc. implications can arise - leading to potentially adverse impacts on brand, image and reputation - which if serious enough can put the airline out of business - temporarily or permanently

Conversely, the in-flight catering disruption is relatively 'low key' in terms of adverse impacts, in that adequate ** BC tactical treatments (see bullet point list below) are readily and relatively quickly available which, when combined with a good communications service (to stakeholders / other interested parties - particularly passengers), should result in 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 e.g. for the in-flight catering situation the airline could typically look at any / all of:

- ** 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
- ** Asking 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** / 'significant period' (and thus, in turn, the associated **RTO**) calculated for the call centre must be quite short - whilst that for catering might be considerably longer





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.' Consequence categories' and 'impact criteria' (see pages 155 to 162) should be standardised (insofar as is possible / practicable) between the RA and the BIA - thus providing a degree of desired consistency between them
..... more on this in **Section 5 / 2B**

Note 2 - most business continuity concepts, associated 'literature' and practitioners refer to 'risk assessment' as being part of the 'understanding the organisation' process. However, pedantically speaking the term we should be using here is 'risk management' - of which 'risk assessment' is just a component part - see Glossary for more details

'Pure' risk management is the practice of systematically identifying and understanding risks to an organisation and the controls that are (or will eventually be) in place to manage them

Ultimately the process gets you to a 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) its (usually adverse) potential impacts and / or likelihoods of occurrence - again, as related to the specific activity / function etc. in question

The risk management process is typically designed so as **not** to encourage organisations to be risk averse. On the contrary, said process 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 adequately balancing risk and reward opportunities

A 'risk averse' culture within an organisation creates inflexibility and can put barriers in the way of achieving the organisation's business objectives. Alternatively, the unthinking acceptance of disproportionately high risk can have significant, adverse impacts on the organisation

Specifically from the BC viewpoint only, risk management techniques are used to **evaluate** the **probability / likelihood** (estimated likely frequency / rate / chance of occurrence) and estimated / predicted * **impact(s)** of **specified threats** - which could potentially cause disruption to an organisation's key product / services etc. (via disruption to the latter's associated key main and key supporting activities etc. also) - 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 continuity management** (in its own right for the latter) take their **impact** levels **instead** - from those found during the associated **BIA**

This evaluation is typically facilitated using a 'Risk **Probability** vs Risk **Impact** Matrix' (see figure 8 - page 138) - 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 (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 occur (be realised)

The '**likelihood / probability**' of the particular risk occurring to the particular activity (**an output of the risk management (assessment) process itself**) forms the other arm of the RA matrix

Based on analysis of the resulting matrix, appropriate 'risk treatments / controls' are formulated to 'manage' the risk. These 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, the organisation's 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 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 'treat / control' the risk **after** it has actually occurred typically by using **BC & 'similar measures'** (emergency / crisis response planning & business **recovery** operations [in contrast with business **continuity** operations] being examples of a '**similar measures**')

Note that the risk treatments identified in the first four bullet points immediately above are '**pre-emptory**' i.e. they are applied **before** an associated threat is potentially realised. The last bullet point (apply **BC** measures) is the only risk treatment applied **after** the threat has been realised - and also the only treatment which has time considerations to account for (i.e. MTPD and RTO)



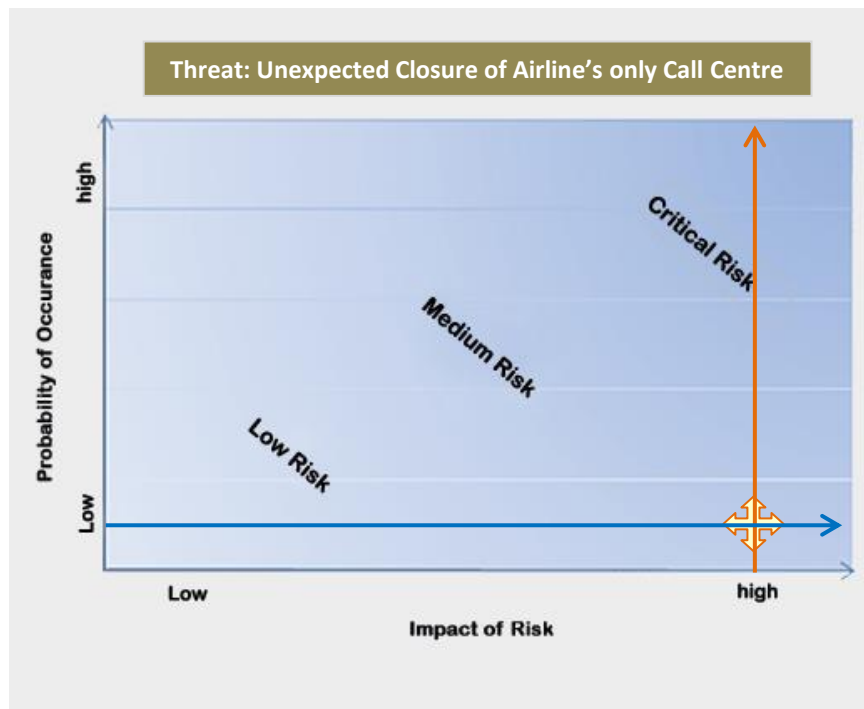


Figure 8 - Simplified example of a very basic Risk Matrix

Note 1 - in the above risk matrix, the adverse **impact** is rated as high whilst the rating for **probability / likelihood** occurrence is low. In such circumstances it is almost certain that such risk would be acceptable to the airline, **provided that** the risk is capable of being actively managed (mitigated) as a * high priority action - 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 treatments / controls after** the risk has been realised [actually occurred]). If it is not possible (for whatever reason) to actively manage the particular risk as described - it should be avoided. The most obvious way to achieve this is to stop the activity

* 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, 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 will neither receive the same priority for treatment (nor the same degree / extent / expense of treatments) as the call centre example

At a simplistic level, the following 'priorities for action' relate respectively to 'high', 'medium' and 'low' risk management (risk assessment) results:

High Priority Action (H) - Implement highly robust controls / treatments as soon as possible

Medium Priority Action (M) - Implement robust controls / treatments within a reasonable timeframe





Low Priority Action (L) - Accept the level of risk and / or..... implement basic controls / treatments at some appropriate future time

Note 2 - examples of risk treatments which can be applied **before** the risk occurs (e.g. in the call centre scenario used in the matrix above) 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)
- Establishing appropriate security to prevent unauthorised access (e.g. by terrorists; by environmentalists etc.)
- Establishing a robust ICT security system

Examples of pre-planned and pre-prepared risk treatments which can be applied **after** the risk has realised (i.e. these are typical **** BC tactical treatments** [controls]) might include:

- Very rapid activation of a 'hot' facility
- Use mobile phones (permanently on charge), email and other manual workarounds. (Mobile phone and email information publicised via airline's main website)
- Work from home i.e. some type of 'virtual call centre'
- ******* Use an outsourced call centre service

****** - the use of BC Tactical Treatments will be covered in **Section 5 / 3** of this guideline

******* - this particular option requires staff at the outsourced call centre to have an adequate level of pre-established competence in place - together with access to the appropriate, operating software. Whilst this option **can** work it is probably going to be quite expensive!

Reminder - 'pure' risk management is only concerned with risk **likelihood** & potential **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's e.g. 'injuries', 'financial loss' and 'reputation damage' etc. - are not risks.....they are **consequences** of realised risk





NOTE - Risk Management

Where an organisation does **not** 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 such responsibilities to be fulfilled

Whilst it is undoubtedly desirable for the larger and / or more complex organisations (such as some 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 in many (if not most) 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 due 'overload'

Exceptionally, an incumbent and very capable 'emergency / crisis response planning manager' might be considered suitable for taking on additional BC accountabilities. Same 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. have a large emergency / crisis response (or similar discipline) business unit (say 4 to 5 persons) - then it may be reasonable for Emergency / Crisis Planning, BC Planning and Risk Planning 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 countries [states]) to comply (mandatory) with the requirements of something known as the ICAO 'safety management system - **SMS**' programme

Risk Management forms a significant part of the ICAO SMS. Accordingly, it is more than likely that for many aviation related organisations today, a fair degree of risk management work (*including risk analysis / assessments*) **will have already been completed** for 'operational safety' matters - typically accomplished by e.g. the organisations' safety and / or quality departments / business units. This information will obviously be of some use for BC (Understanding the Organisation) purposes

However, do remember that BC also applies to matters which fall outside of the ICAO SMS scope. Such matters must also be accounted for in the BIA, RA etc.

See also / again Preamble Note 6 - starts page 7





The (BC Requirements) - Resources Analysis - see also Sub-sections 4 / 1.9; 4 / 2 and 5 / 3.5

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 latter’s component processes and interdependencies] etc.) to pre-defined levels (**MBCO**) within pre-defined timescales (**MTPD** / **RTO**)

The purpose of this analysis is to collect *initial / outline* (‘educated best guess’) 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 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 associated ‘BC Tactical Treatments’

* See Sub-section 5 / 3 / 5 - 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 22301 accomplishes this in clause 8.3.2 as part of formulating BC Strategy) why waste 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 the assignment of resources - especially people) before committing to action





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 **risk** treatments

It further indicates that **one** (*but only one of several*) of the risk treatments available (i.e. '**reduce impact(s)**' - chosen if appropriate to the results of the 'understanding the organisation' task) relates to employment of appropriate **BC measures** (Reminder - the latter ['appropriate BC measures'] are **managed** by the setting of an associated '**BC Strategy**' - and **implemented** by selection of the most appropriate BC 'controls / measures' - otherwise known in this guideline as '**BC Tactical Treatments**')

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 the Incident Response Structure (IRS)
- Producing Business Continuity & Business Recovery Plan(s) - 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 the diagram that the BIA and RA appear to be completed at the same time. This has only 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 will be the same for any set of given circumstances

There are efficiencies to be made if the BIA and RA **are** conducted concurrently i.e. merged. This is because the same subject matter experts providing input to the BIA are the same persons who will provide 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 - some aviation related organisations will have already completed **some** of the risk related work required in the 'understanding the organisation' task - as per the boxed note (last 3 paragraphs) on page 140

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



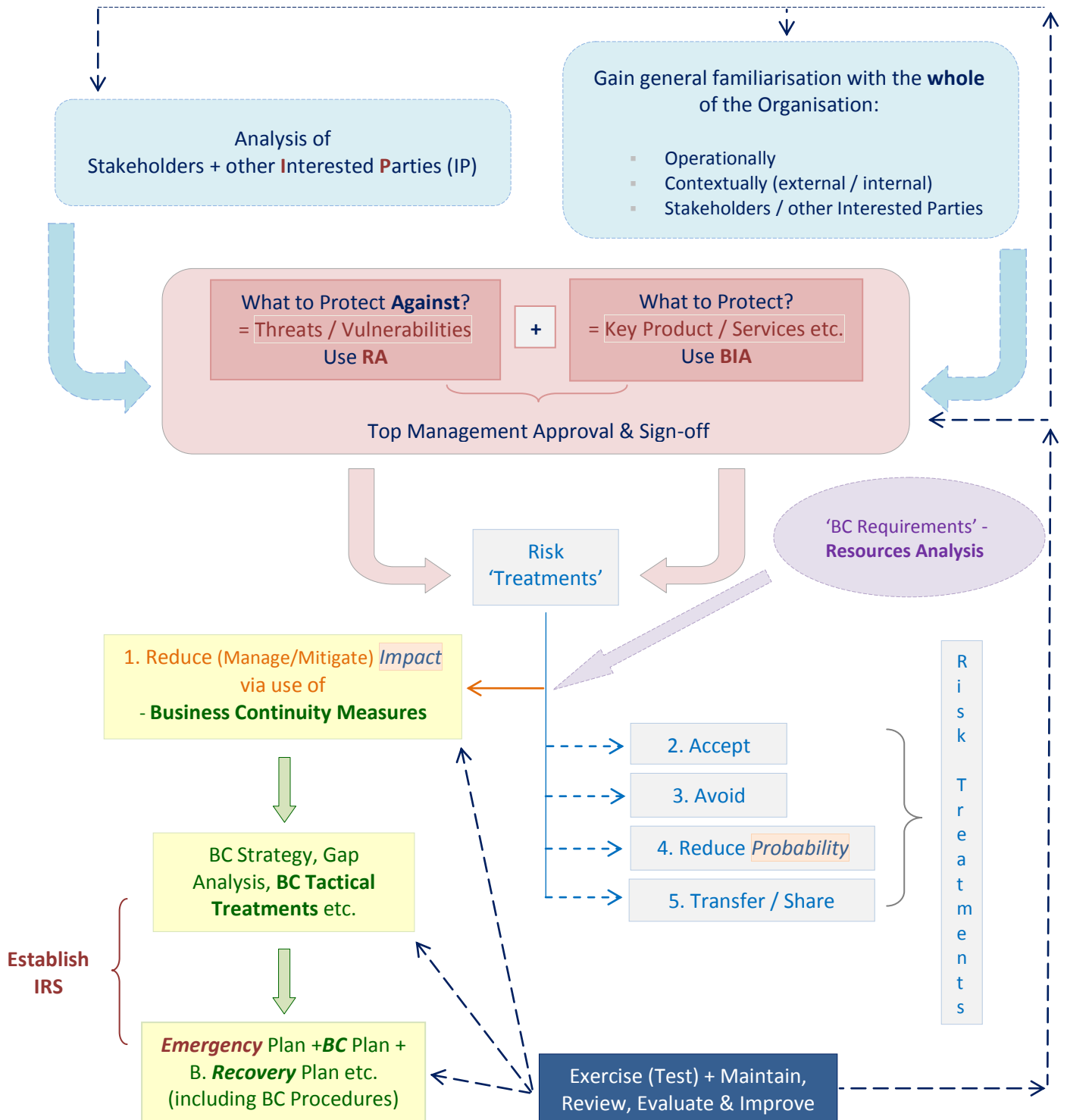


Figure 9 - **Understanding the Organisation** i.e. → IP Analysis → BC Requirements Resources Analysis → BIA → RA → Risk Treatments → BC Strategy → BC Tactical Treatments → BC Plans & Procedures
..... → IRS ← Exercise (Test), Maintain, Review, Evaluate & Continually Improve





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

Note 1 - it is **important** for the user / reader to clearly understand that what follows in this Sub-section 5 / 2B is provided at a 'working overview' level only e. g. the BIA and RA alone for a medium to large sized organisation can take many months to plan for, implement and complete (depending on the required scope of course). The task can also be quite complex

Whilst what is provided herein is essential information by way of understanding these processes at an overview level - further guidance will be required in reality - unless the user / reader is already competent / qualified / experienced in the appropriate BC and Risk Management matters

There are quite a few resources available to at least address the 'qualification and competence' requirements mentioned above (via internet; books; by taking commercially provided training etc.) - almost all of which require purchase

The 'experience' requirements will need to be gained / earned in the usual way i.e. hands on familiarisation over a suitable period of time, under the watchful eye of someone who already has such appropriate competence, experience and possibly (preferably) qualification

A limited selection of such resources has been included starting on page 199. Recommended reading to start with includes the Western Australia government's documents (one for Business Continuity - the other for Risk Management) and the handbook referred to on page 201 (latter requires purchase)

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 set, approved, 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. - make themselves appropriately available and 'co-operative'

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





Section 5 / 2B / 1

Stakeholder / other Interested Parties Analysis

The method of accomplishing the 'stakeholder / other interested party' analysis has already been described in [Section 5 / 2A](#) & [Section 4 / 1.5](#)

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 if necessary

A review of figure [10](#) on the next page is also recommended - in order to better understand the relationships between the various terminologies used - as related to BIA task:

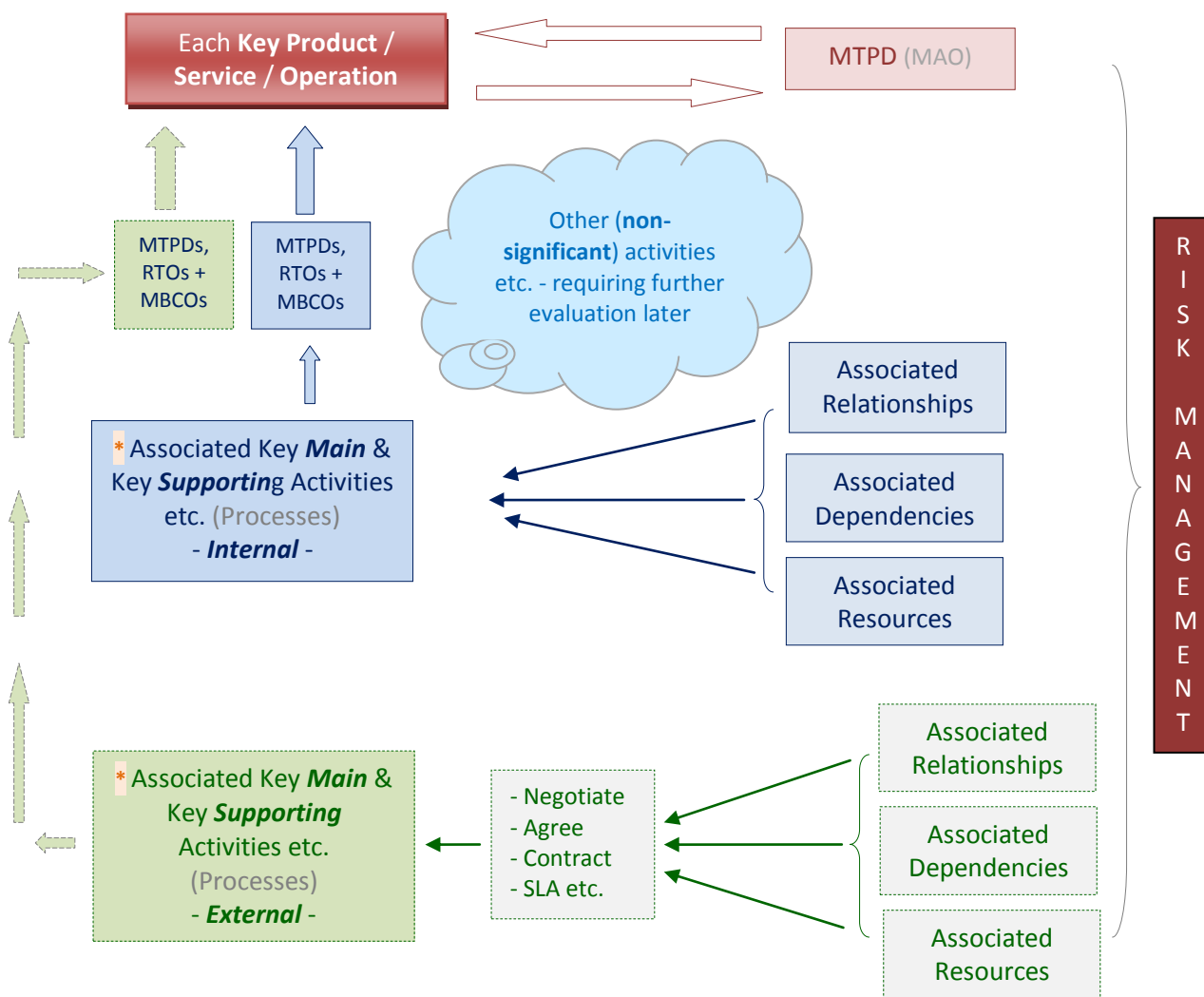
IMPORTANT NOTE - a BIA typically works on a worst case scenario, generally based on the concept that the impact of a significant disruption event on a particular activity - leads to the *complete cessation* of that activity





Figure 10 - BIA - Indicating relationships between:

Key Product / Service / Operation → Key Activities etc. → Interdependencies → Resources



- * = Activities, processes 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'





Business Impact Analysis / *continued*

As already mentioned, the BIA is an essential starting point for developing BCMS within an organisation. Outputs from the BIA typically lead on to everything else associated with managing the impacts of disruption e.g. the setting of BC strategy; the formulation (within the BC strategy) of BC Tactical Treatments (control measures); the production of the associated 'system' and plans which will enable all of the aforesaid to be accomplished; tentative identification of the appropriate resources required etc.

Get the BIA wrong and the chances are that the BCMS which is eventually developed will inadequately provide for the business continuity requirements of the organisation

As assessing the potential *impacts* of a significant disruption event on an organisation is inherently subjective in nature, the BIA process attempts to reduce such subjectivity (to some degree at least) by providing a *consistent* set of *rules* (methodology) and *measurement criteria* - which should be applied (across the organisation) throughout the BIA

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 who are to supply the BIA inputs (subject matter experts 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 - it is assumed herein 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 further below

2. Top management to approve (in principle at this point) provision of the estimated resources (including internal personnel resources and budget) likely to be necessary *to conduct the BIA*
3. Complete appropriate *preparations* e.g.
 - Establish and document the *scope* and *context* of the BIA and how it will be *practically conducted* (methodology & supporting BIA procedures). Include here details of the planning & co-ordination processes to be used for the associated data gathering and analysis tasks





- Identify, document and establish the BIA *consequence categories* to be used (see page 156)
 - Identify, document and establish the BIA *criteria* to be used when *quantifying* and / or *qualifying* the *impacts* and the associated *timescales* (over which such impacts might be assumed to act) (see page 160)
 - *Prepare & document a reasonable number of appropriate, 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 in item 8). 'Worst case' (but nonetheless reasonably realistic) scenarios should typically be used for this purpose
4. Ascertain & document the resources required (necessary to conduct the BIA itself) and by when they should be available
5. Identify organisation's *key product(s) / services / operations*

Identify, 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] related *scoring system* to assess *priority* - the latter being appropriate to the continued functionality of such key product / service / operation to the organisation - in the event of same being adversely impacted by 'significant disruption' over a 'significant period' of time). The results of the 'Stakeholder / other Interested Party Analysis' will assist in this task

(* as defined in 'criteria')

6. Obtain top management's *agreement & approval* to outcomes of items 3, 4 & 5 above
7. Obtain and / or facilitate use of the various (already identified and now approved) *resources* required to conduct the BIA
8. *Collect, document and analyse the required data*

Generally conducted by means of any / all of workshops, questionnaires, interviews & similar - *being targeted specifically at those (subject matter experts) within and outside the organisation best able, qualified and experienced - to provide the required information, data etc.*





For example and as a general guide:

- **Interviews** (one on one or similar concept) can provide **good** quality information / data - but are typically time consuming / work intensive. The interviewer can directly control (to a degree) what is provided (including the level of detail + its relevance and consistency)
- **Questionnaires** may (repeat may) provide large amounts of data in quick time - but the reliable return of completed documents can be problematic and the information / data provided can be of **poor** quality, be inconsistent etc. - if the associated methodology is not adequately managed
- **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?)

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 **MTPD** for **each** identified **key product / service / operation**
 10. Obtain top management's **agreement & approval** to outcomes of items 8 & 9 above
 11. Make further use of analysed data to complete and document items 12 to **22** below:

Note 1 - a 'process mapping' analysis (see Glossary) might be found useful to facilitate what follows. **Note 2** - see item **21** further below **now** i.e. before carrying on with item 12
 12. For **each** identified **key product / service / operation** - further identify and document the appropriate, associated (subordinate) **key main activities**





Identify, document & prioritise **each** associated **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** - the latter being appropriate to the continued functionality of such key main activity - in the event of same being adversely impacted by 'significant disruption' - over a 'significant period' of time)

* As defined in BIA 'criteria'

** 'Score' each result in 'units' of **impact assessment** (for eventual input into the **risk management** (assessment) matrix [see examples in figures 11 to 17, pages 163 to 171]) and in terms of '**priority for action to be taken**' (e.g. 'highest', 'high', 'medium', 'low' and 'for possible future attention')

Key main activities internal and external to the organisation shall be accounted for

13. For **each** key main * **activity** identified in 12. above (and in the 'scored' priority order) - estimate and document an appropriate **MTPD** and **initial RTO** - such that the MTPD estimations are ** compatible (i.e. equal to or shorter) with the **MTPD** of the associated (**parent**) **key product / service / operation**

Where such **MTPDs** and **RTOs** relate to external organisations - estimation and application of same will need to be negotiated and agreed with such external organisations - e.g. via contractual 'service level agreements' 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**. For the sake of simplicity and brevity the latter are generally ignored herein. However, when conducting a BIA **in reality**, all such processes (as associated with **key main activities** as per this item 13.) 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

** Note - where a **key main activity** MTPD estimated as per above is **longer** (in terms of time) 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** - further identify and document the appropriate, associated (subordinate) **key supporting activities**





Identify, 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** - the latter being appropriate to the continued functionality of such key supporting activity - in the event of same being adversely impacted by 'significant disruption' - over a 'significant period' of time)

* As defined in 'criteria'

** 'Score' each result in 'units' of **impact assessment** (for eventual input into the **risk management** (assessment) matrix [see examples in figures 11 to 17, pages 163 to 171]) and in terms of '**priority for action**' (e.g. 'highest', 'high', 'medium', 'low' and 'for possible future attention')

Key supporting activities internal & external to the organisation shall be accounted for

15. For **each key supporting *** activity** identified in 14. above (and in the 'scored' priority order) - estimate and document an appropriate **MTPD** and **initial RTO** - such that the MTPD estimations are **** compatible (i.e. equal to or shorter) with the **MTPD** of the associated (parent) **key main activity**

Where such **MTPDs** and **RTOs** relate to external organisations - estimation and application of same will need to be negotiated and agreed with such external organisations e.g. via contractual 'service level agreements' or similar

*** Reminder - from the glossary meaning of the term '**activity**' as used herein, most (if not all) **activities** typically comprise of a series of associated **processes**. For the sake of simplicity and brevity the latter are generally ignored herein. However, when conducting a BIA **in reality**, all such processes (as associated with **key supporting activities** as per this item 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

**** Note - where a **key supporting activity MTPD** estimated as per above is **longer** (in terms of time) 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 also) addressed in items 12 to 15 above - identify all **associated and appropriate dependent / inter-dependent** matters





Document each such dependency / inter-dependency which is 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 'criteria')

17. Analyse the results of item 16. Where so required *adjust all initial RTOs* from items 13 & 15 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

18. Decide, assign and document the *MBCOs* to be achieved when disrupted activities are assumed to 'resume' at the associated RTOs
19. Identify and document '*single points of failure*'
20. Use *impact* level assessments (scores) from items 12. and 14. above as *inputs* to the *risk management (assessment)* process
21. Whilst conducting items 12 to 17 above - also identify and document those internal and external activities (+ their associated processes) which, whilst not having been allocated a significant priority (score) level, *are nevertheless 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 is worthy of re-consideration for inclusion in the BC strategy / tactical treatment process *OR* possibly 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 the other three components [business tools] of the 'understanding the organisation' process and approved by top management) **will be used in due course to formulate an associated * 'BC Strategy'**

* It will be recalled that the BC Strategy, in turn, outlines [from the higher level viewpoint] what the organisation needs to achieve going forward from (after) the BIA - in order to try to ensure continuity of its key activities etc., following a significant disruption event to same e.g. formulation of '**BC Tactical Treatments**', setting up of the '**Incident Response Structure**', production of the associated **BC Plans** etc.





Notes regarding 'BIA' Points 1 to 22 above (in no particular order)

Training (Familiarisation)

Further to item 8 above, it will 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) will be of significant overall benefit to the BIA 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

'Owners' of Key Main Activities / Key Supporting Activities / Dependencies

For items 12, 14 & 16 above, also identify and document the 'owners' (persons directly responsible for) of the activities & dependencies. 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) impact is acceptable to specific revenue generating activities

They will also be able to provide advice to the Business Continuity Manager on the formulation of appropriate (financial) 'consequence categories'(see figure 11 / page 163)

Item 16 - Dependencies

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.) and its associated power sources (mains electricity, UPS, generators etc.)

Calculation of RTOs

In this guideline document the calculation of RTOs & MBCOs is made here in **Section 5 / 2** - as part of the 'understanding the organisation' task i.e. as a result of the BIA. Other 'schools of thought' assign RTOs etc. in the 'Setting BC Strategy' task which follows on. In the final outcome, the choice of *when* to assign RTO etc. makes no significant difference in theory. From a practical / logical viewpoint, however, RTO assignment during the BIA does have its advantages





BIA - Outcomes

The outcomes from a Business Impact Analysis should have typically provided:

- A list of 'in-scope' key products / services / operations (typically prioritised in terms of disruption impact on significant factors - including direct / indirect revenue)
- A list of key main activities & component processes (internal and external & similarly prioritised) - which contribute to the delivery of the related key products / services / operations
- A list of key supporting activities & component processes (internal and external & similarly prioritised) - 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)
- Impact inputs for the associated risk assessment procedure
- Documentation related to 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 141])

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 fully understand the strategic 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) - arrange a workshop(s) with senior executives from key areas of the organisation, in order to complete this step 1. Additionally, 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 all done, confirm / obtain agreement & approval from top management on the strategic objectives of the organisation, ensuring that they are concisely defined, measurable and accountability is allocated for each

Step 2

Methodology

Already covered further above (pages [145-153](#))

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*. Examples of such criteria might typically include (the list is not exhaustive):

Criteria - Consequence Categories - General

The term '**consequence 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 particular risk (threat) occurrence, might (**as a consequence**) have a significant impact(s) on the ability of the organisation to deliver said key product / services / operations

Consequence Categories must be specific to the organisation **and** activity to which they are to apply

Examples of some generic consequence 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 'safety' and '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 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*' of disruption to different activities within 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). You are reminded that this list is not exhaustive

- Consequences - 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 - 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 to cash flow
 - Impact to market share
 - Impact on future sales
 - Impact on stock market share price
 - Contractual fines and / or penalties
 - Lawsuits
 - Loss of financial control
 - Bankruptcy
 - Cessation or limitation of operation
- Consequences - 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 for those deemed culpable)
 - Cessation or limitation of operation





- Consequences - 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 - 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 - 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 - Environmental Damage (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 'consequence's e.g. 'injuries', 'financial loss' and 'reputation damage' etc. - are not risks.....they are **consequences** of realised risk





*Criteria - Consequence Categories - Expressed **Qualitatively** and / or **Quantitatively***

Consequence categories may be expressed qualitatively, quantitatively or as a mixture of both

As an example let's take 'customer related considerations'. '**Qualification**' type units applied to the latter (in terms of adverse impact) might be as simple as 'low - medium - high' or, a little more exacting, expressed e.g. on a scale of '1 to 5' where 1 might = 'very low impact' whilst 5 might be 'catastrophic'

'**Quantification**' units for the same example might be 'lose 10% of customers within * 24 hours; 25% of customers within 48 hours; 50% of customers within 5 days and 90% of customers within 7 days

(* Note here that we have added an extra dimension to the quantification impact assessment i.e. **time** [more of the latter a little further below])

Generally speaking, qualification units are more appropriate to smaller / simpler organisations whilst a mix of qualification and quantification might better suit the larger / more complex organisation e.g. 'financial impacts' are typically better expressed in terms of quantification units - whilst 'brand / image / reputation' impacts may be better expressed by qualification or by a combination of qualification and quantification

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 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

A 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 lost during a significant disruption event

A good 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 these should be recorded, combined and considered to try to give an idea of what the worst case financial impact(s) might be





Criteria - Consequence Categories - The 'Time' Factor

Disruption planning and the application of associated BC countermeasures (BC Tactical Treatments) are usually inextricably linked by **time** e.g. when will the effects of a disruption start to impact adversely on an organisation's key activities etc. - and when does this impact become significant to the degree of becoming unacceptable - and, consequently, when does the organisation need to invoke / activate its 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 - 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 regard to the time when the disruption first commenced (see pages 163 to 171 for examples)

Such 'unacceptability' regarding time-sensitive activities might need to be specified e.g. to the minute or the hour. Less exacting accuracy will be acceptable for less time-sensitive processes e.g. days, weeks, even months or longer - the rebuilding of a destroyed office facility being an example of the latter. And to re-iterate, some activities, regarded as critical, do not pedantically have a time-sensitive limit for resumption, other than 'immediate' - again, using here the example of a 'surgical operating theatre'

Criteria - 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 'catastrophic / near catastrophic'

* **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 regard to **impact**:

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 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 for days or perhaps a week, but eventually restoration of the resource 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 of a disruption event upon a specified activity / process - 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

Criteria - Priority

Activities which are subject to a significant impact as a result of a significant disruption event need to be assigned a priority regarding 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 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 [likelihood / probability] coming from the *risk management [assessment]* process - as will be seen a little later)

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 Criteria' is a totally different subject to BIA related activity 'Priority Criteria' - don't get confused between the two

Criteria - Examples

Some examples of how 'criteria' might be applied during a BIA are shown on pages 163 to 171

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). For the latter (in reality) it will be necessary to derive consequence categories which are 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 level - represented (**priority** criteria) by the number '1'. However, **other** activities within 'ABCX Airways' will (almost certainly) 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 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 14-17 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 notes 1 and 2 on page 171 **before** reading further





EXAMPLE ONLY - Fig 11

Generic *BIA Reference Matrix* - used to formulate **impact criteria** (which in turn are used to provide impact adversity 'scores' for specified activities - see Fig 12)

CONSEQUENCE Category →	Interruption	Op. Efficiency	Regulatory etc.	Financial	Reputational	Stakeholder	Injuries etc.	Other
IMPACT Criteria ↓								
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'] - latter would have been derived from [separate] RA)

<i>Impact Parameters</i> ↓	<i>Impact Durations</i> →	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
<i>Assessment of overall impact of activity loss</i>		2	2.5	3	3.5	4

Impact assessments - graded ('scored') by degree of adverse impact

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 estimated impact 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'] - latter would have been derived from [separate] RA)

Impact Durations →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
	↓	↓	↓	↓	↓
Assessment of overall impact 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 estimated impact 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 - latter would have been derived from [separate] RA)

<i>Impact Parameters</i> ↓	<i>Impact Durations</i> →	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
<i>Assessment of overall impact of activity loss</i>		2	2.75	3.5	4	4.75

Impact assessments - graded ('scored') by degree of adverse impact

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 estimated impact 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. - latter derived from [separate] RA)

<i>Impact Durations</i> →	6-24 hrs	24-48 hrs	2 to 4 days	4 to 7 days	7 days +
	↓	↓	↓	↓	↓
<i>Assessment of overall impact of activity loss</i>	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 estimated impact 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 - latter derived from [separate] RA)

Impact Durations →	None Acceptable				
	↓	↓	↓	↓	↓
Assessment of overall impact of activity loss	4.9				

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 estimated immediate impact = **4.9**





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 - latter derived from [separate] RA)

Impact Durations →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
	↓	↓	↓	↓	↓
Assessment of overall impact 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 estimated impact 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 - latter derived from [separate] RA)

Impact Durations →	1-2 hours	3-6 hours	6-12 hours	12-24 hours	24-36 hours
	↓	↓	↓	↓	↓
Assessment of overall impact 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 estimated impact beyond 30 to 36 hours outage = **4.25**





Note 1

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])
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 here. In reality they must be identified and accounted for)
Interdependencies (External): = TBA (Note - these have been ignored here. In reality they must be identified and accounted for)

Note 2 - **VERY IMPORTANT**

At the bottom of each of figures 12 - 17 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 as shown immediately above) is the one that you will use during the associated **risk management (assessment)** procedure (see Section 5 / 2B / 3). 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 procedure itself)





BIA - Review & Evaluation

Good practice dictates 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

The BIA process should not be repeated in its entirety at review e.g. only those key products / services / operations / activities / processes / dependencies and resource sources 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 - before restarting the sampling cycle again





Section 5 / 2B / 3

Risk Assessment

See again Notes 1 & 2 on page 136. Also see *risk related* definitions now - pages 176 to 178

Reminder 1 - Risk Assessment is a component of the overarching Risk Management process

Reminder 2 - Risk Management versus Business Continuity (see next 4 paragraphs)

It will be recalled that risk management is simply the practice of systematically selecting cost-effective approaches for minimising the effect of threat realisation (i.e. of a threat actually occurring) to one or more of an organisation's activities. Threats can never be fully avoided or mitigated due various types of practical limitation. Therefore, all organisations need to accept some level of risk

Whereas risk management tends to be pre-emptive, business continuity management (BCM) was 'invented' to deal with the consequences of a realised threat(s) - i.e. *after* the threat has occurred

Risk management and BCP are often mistakenly seen as 'rivals'. In fact, the two are so closely interwoven that such separation is almost academic. For example, the risk management process can create important inputs for BCM (e.g. identification of assets [resources such as people, equipment, facilities etc.], threat impact assessments, cost estimates and so on)

Risk management also proposes applicable controls (treatments) for identified risks - one of which *might* be BC. Therefore, risk management covers several areas which are vital for the BCM process and even (in fact) for its existence. However, the BCP process goes beyond risk management's *pre-emptive* approach and assumes that the 'disruptive incident' *will* actually happen at some point - and so 'what happens then / what do we do now'?

General

To re-iterate, risk management tries to identify and manage 'what you are protecting your organisation against' i.e. threats (and the associated vulnerabilities of what it is [within your organisation] that they threaten) - and how best to deal with them

Typical threats include those which have the potential capability to:

- 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 etc.
- Cause loss of systems, networks and similar scenarios
- Cause failure of key supply systems etc.
- Damage brand / image / reputation
- etc.





Each organisation should identify and document the threats which it believes might have both a sufficient **impact** (on itself - or more specifically on its business activities, processes, resources, dependencies [including suppliers] etc.) to be worth considering in the first place..... **and**, additionally, also have a sufficient degree of **likelihood / probability** of occurrence at some unspecified future time

Identified threats (to specified activities, processes resources etc.) should be regularly **reviewed** in order to check the validity of already assigned likelihood and impact assessments

Such reviews also need to look for and add any new threats. For example, it is only fairly recently that many organisations (including airlines and airports) have needed to account for the threat of communicable disease in the form of pandemic (most specifically - 'avian influenza [bird flu])

Today (2018) 'pandemic' (along with ICT related vulnerabilities / crime, terrorism / sabotage and the 'weather / natural phenomenon' [e.g. global warming {albeit caused by humans}]) is high on most national, regional and local government threat lists (known as **risk registers** - [more on how / why the word 'threat' has changed to 'risk' here will be covered at the top of page 177])

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 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 will also be typically 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

* **Note** - 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

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 shall assume this herein) that the specific **risk** control / treatment (which should relate directly to the application of **BC** measures) has either not been addressed at all - or has been addressed in an inadequate manner (if this was **not** the case then the RM department / business unit [if it exists] has, 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 into the BC 'understanding the organisation' task. For example, the RM unit may have missed out some key activities from its own 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 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 unit itself. It is these 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 note' at bottom of page 171

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 will now probably require urgent attention!

Lastly, it will be recalled that 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**'!). It is possible that such operational risk assessments might be undertaken by an organisation's RM department / business unit (if it has one?). However, they are far more likely to be undertaken by the organisation's safety manager or equivalent. Regardless, the results are available for use (**and should be so used**) in the appropriate parts of the **BC** 'understanding the organisation' task

IMPORTANT - if there is no formal RM capability within an organisation, top management should decide on and approve (including budget where required) an appropriate course of action. Some of the options might include:

- Establishing a formal RM department / business unit in its own right (which may or may not **also** be required to formally handle BC matters in full)
- Assign RM duties (purely as they impact on formal BC matters but nothing else) to the BC department / business unit. This effectively means that **other** required RM capabilities will not be available to the organisation
- Appoint an external 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)

A threat 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 almost 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 on page 179

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 no alarm system; lack of fire extinguishers; no other fire suppressant system(s) (e.g. sprinklers); no fire doors; 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 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, 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 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** - and which might (if it occurs) 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 once every 20 years (e.g. as might be extrapolated from statistical meteorological data for a 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

 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**')

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 controls** (treatments / measures etc.) **put in place to manage same.** **This process ultimately leads to the point of deciding 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 selection 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. 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 are included (per threat) for consideration - as applicable
- The next text box to the right indicates (for some of the threats & thus for example purposes only) just some of the typical *consequences* should the threat be realised (see also 'RA Triggers' page 184)
- Space constraints on the next page have prevented insertion of the potential *vulnerabilities* which are typically associated with each threat. However (and as an example), the threat of fire to a facility is 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 fire drills scheduled etc.





Figure 18

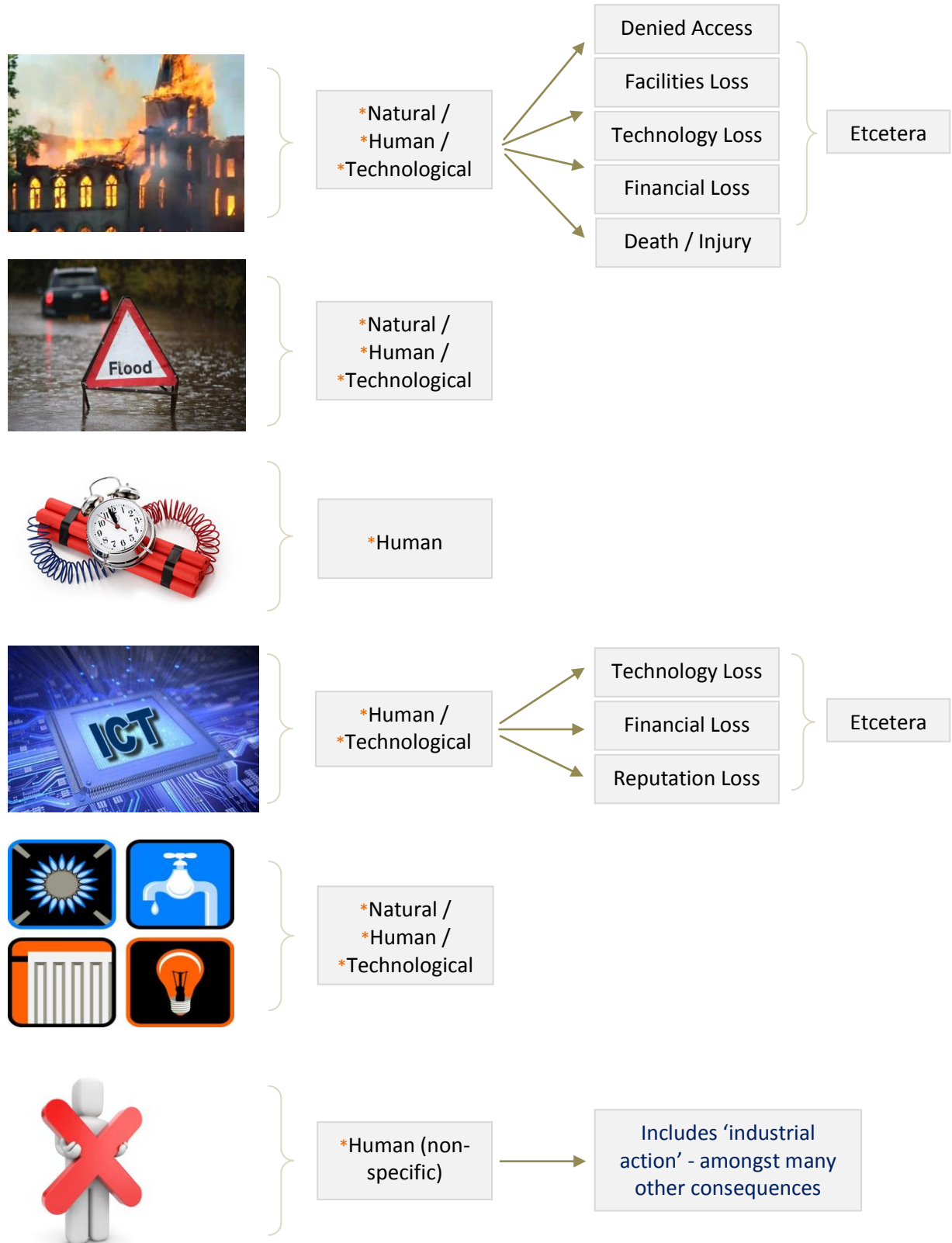
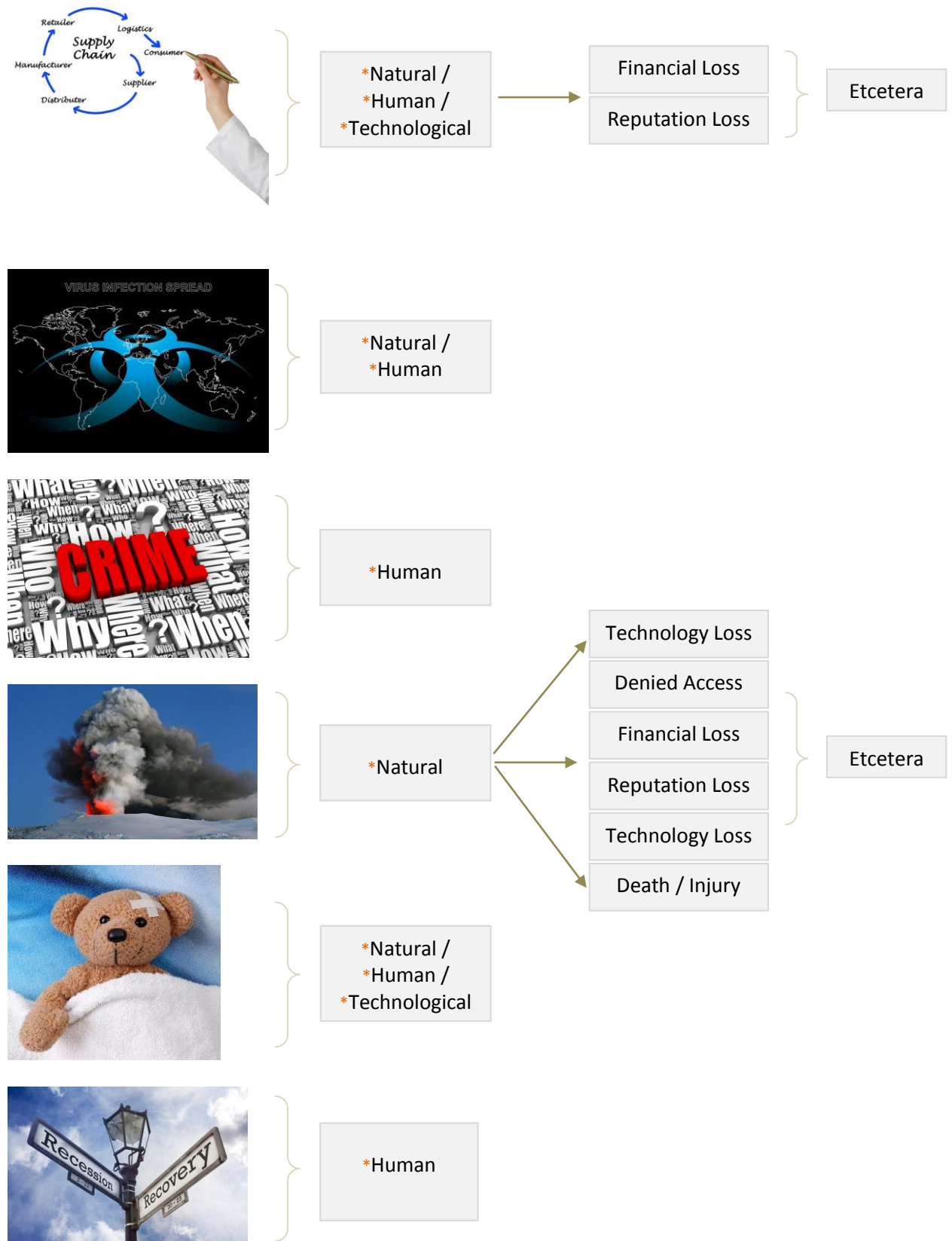




Figure 18 - continued





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 tactics) 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 all of the above
- Cyclically review all of the above
- Retain and maintain documented records where appropriate

* This information will already be available from the 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

Note 1 - see also 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, use the BIA methodology as an approximate template (starts page 147)





Risk Management (Assessment) Process

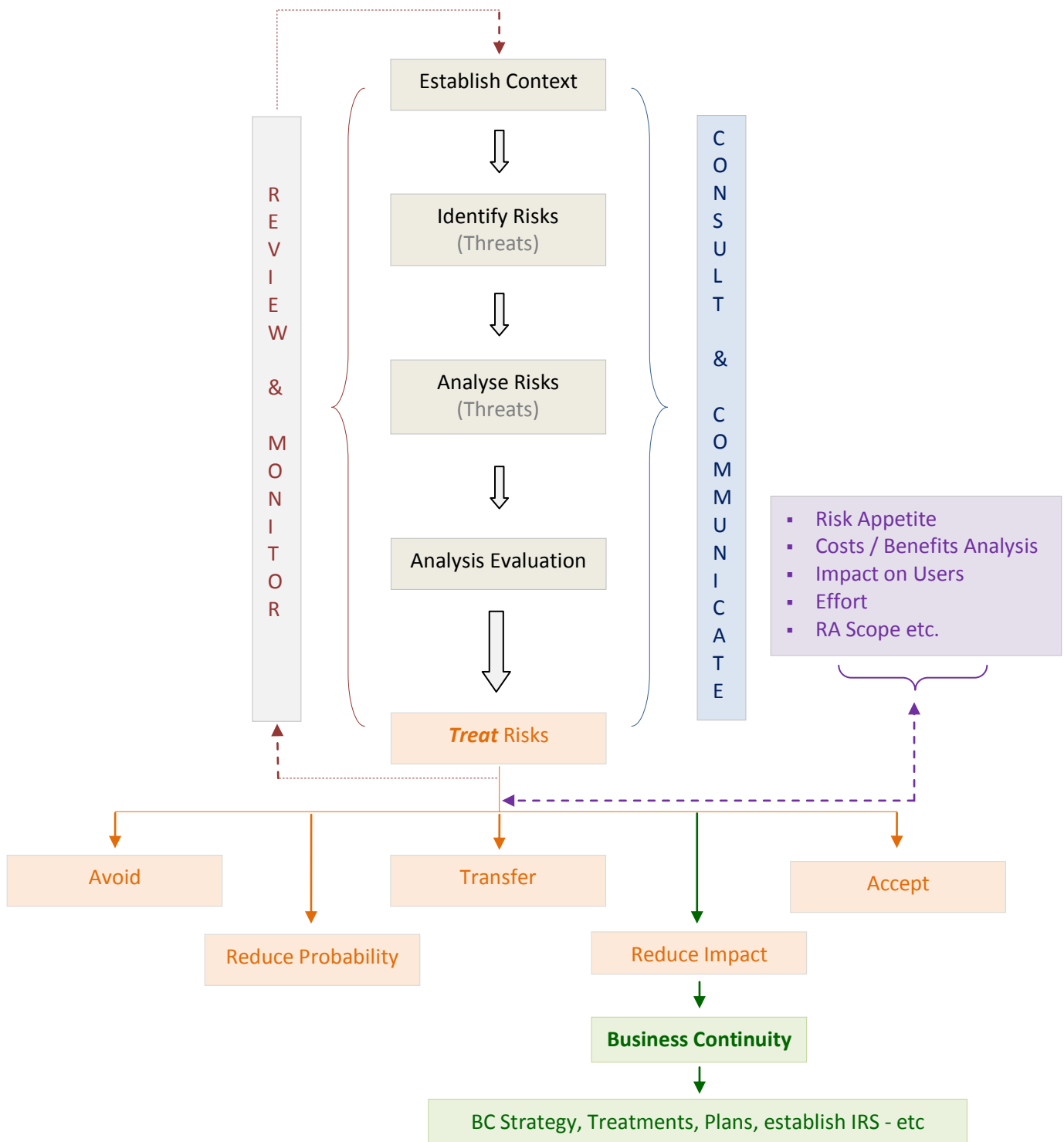


Figure 19





Assessing Risk

There are several methods used to assess (quantify / qualify) risk - none of which is perfect due to the subjective nature of the topic. Perhaps the most widely used method (due to its relative simplicity) uses the following parameters:

Assessed Risk = **Impact** of **threat** event x (multiplied by) **probability** of **threat occurrence**

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 in 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

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 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 short 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 managers (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 treatments / controls resulting from the 'new' RA are then established - and will more than likely (but not always) ** confirm that the 'already in place' controls are still valid / required - and may possibly also identify the need to add additional controls

** 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** controls / treatments have been applied (there will **always** be some such risk) is typically known as '**residual risk**'. The residual risk is generally (but not always) acceptable to the organisation. Should it not be acceptable, further treatments / controls should be applied until it becomes acceptable. If the latter is unachievable, then the activity will probably need to be abandoned

RA Triggers

To better manage and organise the RA process and to facilitate what is to follow on (i.e. selection of appropriate RA controls / treatments - 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 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 usually 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 the results of the BIA

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)

Examples

* We can now look at a generic example (see pages 186 to 191 below) of how the above might work in practice - by taking the subject of ‘operational (safety) risk assessment’ e.g. within an airline, an airport etc. In this example we shall be looking specifically at the aviation related activity known as ‘**safety**’

* Taken from ICAO Safety Management Manual (Doc 9859 AN/474 - Third Edition 2013)

<http://www.icao.int/safety/SafetyManagement/Documents/Doc.9859.3rd%20Edition.alltext.en.pdf>

See page 175 of this guideline document for what type of aviation related organisations typically fall under the umbrella of ‘operational risk management’. The **principles** of operational risk assessment also apply equally to all other activities within the organisation - which are not classified as ‘operational’ e.g. HR, Finance etc.

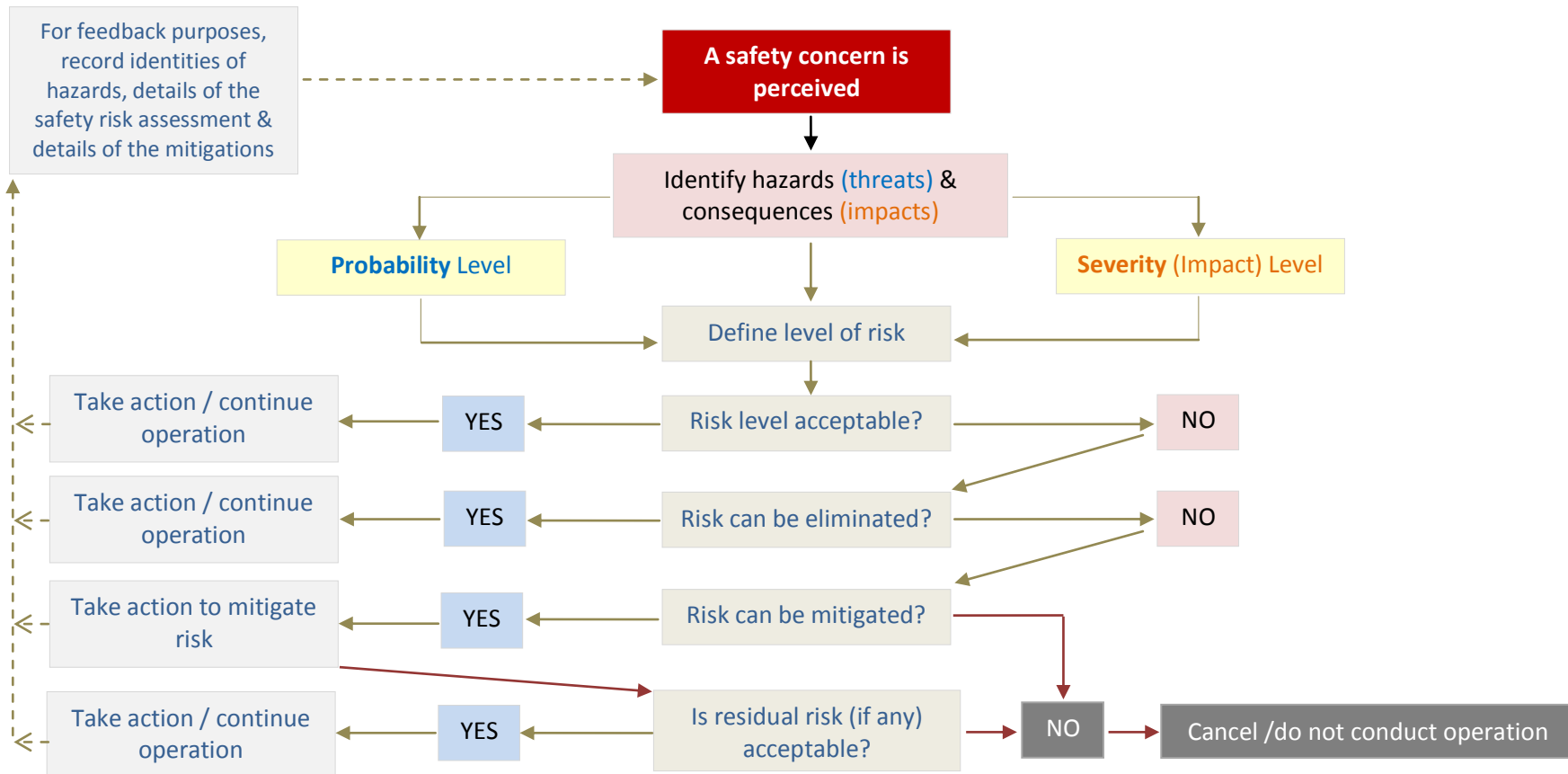
Note - as at 2018, almost all major aviation related organisations need to comply with the requirements of the International Civil Aviation Organisation’s (ICAO) Safety Management System - ‘SMS’, including those related to ‘safety / operational risk management’. A simplistic flowchart of how the latter ‘works’ is shown on the **next** page





Examples

Figure 20A - Operational Risk Management (**Activity = Safety**) (This page © ICAO)





Examples - continued

SAFETY RISK (This page © ICAO)

Safety Risk Management is another key component of a Safety Management System (SMS). The term **safety risk management** is meant to differentiate this function from the management of **financial** risk, **legal** risk, **economic** risk, **reputational** risk and so forth. This section presents the fundamentals of safety risk and includes the following topics:

- a definition of safety risk
- safety risk probability
- safety risk severity
- safety risk tolerability.....and
- safety risk management

Definition - ‘Safety Risk’

Safety Risk is the projected likelihood and severity of the consequence or outcome from an existing hazard or situation. While the outcome may be an accident, an ‘intermediate unsafe event / consequence’ is likely to be identified as the most credible outcome

Safety Risk Probability

The process of controlling safety risks 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 or frequency that a safety consequence or outcome might 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 or components of the same type might have similar defects?
- ❖ How many personnel are following, or are subject to, the procedures in question?
- ❖ What percentage of time is the suspect equipment or questionable procedure in use?
- ❖ To what extent are there organisational, managerial or regulatory implications that might reflect larger threats to public safety?

Any factors underlying these questions will help in assessing the likelihood that a hazard may exist, **taking into consideration all potentially valid scenarios**. The determination of likelihood can then be used to *assist* in determining safety risk **probability**





Examples - continued (This page © ICAO)

The diagram below shows a typical safety risk **probability** table. It includes five categories for denoting the probability related to an unsafe event or condition, the description of each category, and an assignment of a value 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 may include both qualitative and quantitative criteria that may include up to fifteen values

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 of harm that might reasonably occur as a consequence or outcome of the identified hazard.....*' 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 aircraft, property, infrastructure etc. damage?

The severity assessment should consider *all possible consequences* related to an unsafe condition or object, *taking into account the worst foreseeable situation*

The diagram 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. This table is an example only





Examples - continued (This page © ICAO)

Severity (Impact)	Meaning	Value
Catastrophic	<ul style="list-style-type: none">▪ Multiple Deaths▪ Severe Destruction of Property, Infrastructure etc.	A
Hazardous	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ 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	<ul style="list-style-type: none">▪ Nuisance▪ Operating Limitations▪ Use of Incident Procedures▪ Incident (not serious)	D
Negligible	<ul style="list-style-type: none">▪ Few consequences (none serious)	E

Figure 20C - Safety Risk Severity (Impact) Table

Safety Risk Assessment

The safety risk probability and severity assessment process can be used to derive a safety risk index. The index created via the methodology described (in the tables) 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 - in the figure at the top of the next page





Examples - continued (This page © ICAO)

Risk probability	Risk severity				
	Catastrophic A	Hazardous B	Major C	Minor D	Negligible E
Frequent 5	5A	5B	5C	5D	5E
Occasional 4	4A	4B	4C	4D	4E
Remote 3	3A	3B	3C	3D	3E
Improbable 2	2A	2B	2C	2D	2E
Extremely improbable 1	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, it is necessary to obtain the indices in the safety risk assessment matrix. For example, consider a situation where a safety risk probability has been assessed as occasional (4), and safety risk severity has been assessed as hazardous (B). The composite of probability and severity (**4B**) is the safety risk index of the consequence

The index obtained from the safety risk assessment matrix must then be exported to a safety risk tolerability matrix (see [next page](#)) which describes the tolerability criteria for the particular organisation. Using the example above, the criterion for safety risk assessed as **4B** falls in the ‘**unacceptable under the existing circumstances**’ category. In this case, the safety risk index of the consequence is unacceptable. The organisation must therefore:

- Take measures to reduce its exposure to the particular risk, i.e. reduce the likelihood component of the risk index.....and / or
- Take measures to reduce the severity of consequences related to the hazard, i.e. reduce the severity component of the risk index.....or
- Cancel the operation if mitigation (reduction) is not possible

Note. The inverted pyramid in the figure below (next page) reflects a constant effort to drive the risk index towards the bottom APEX (acceptable risk area) of the pyramid





Examples - continued (This page © 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	Description	Recommended Action
5A, 5B, 5C 4A, 4B, 3A	High Risk	Cease / cut back operation promptly if necessary. Perform priority risk mitigation to ensure that additional and / or enhanced preventive controls are put in place to reduce risk to moderate or low range
5D, 5E, 4C, 4D 4E, 3B, 3C, 3D 2A, 2B, 2C	Moderate Risk	Schedule a safety assessment which will be used to reduce the risk to the low range if viable
3E, 2D, 2E, 1A 1B, 1C, 1D, 1E	Low Risk	Acceptable. No action required

Figure 20Fand another model - complete with recommended actions



Examples - continued

In the next example (which is *real*) we are looking at a specific threat against an airline operation

The threat was that of a * sub-sea 'earthquake initiated' *Tsunami* and it 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 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 to where this Tsunami originated

It will be recalled from page 184 that a threat impact of '5' must be managed / mitigated *regardless of* the 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)





Examples - continued

Extract from a typical airline's RISK REGISTER (showing a typical Risk Matrix)

(Wet leased) FLIGHT OPERATIONS 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 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 e.g. 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 above) 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)





Summary Notes re **Risk** Management Procedure described above (in no particular order)

Risk Management Department / Business Unit

For the purposes of this guideline document 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 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 assigned to provide the information required (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 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) - 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 control / treatment plan





- Identification of tactical controls / treatments **for which BC measures are most appropriate**
- Documentation related to all of the above
- Top management review and approval

Consequence Categories

The term 'consequence 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 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 Categories must be specific to the organisation **and** activity to which they are to apply

Examples of some generic consequence 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 'safety' and 'security'

To ensure consistency within an (the same) organisation with regard to the closely associated subjects of **risk** assessment and **business (continuity)** impact assessment, a **common** or near common set of consequence 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 change need to be thoroughly reviewed. For evaluation / audit purposes, same may require periodic 'sample' review & confirmation of previous risk management / assessment





ISO 22313 / OPERATIONS / Risk Assessment - 8.2.3

Please note the following extract from ISO 22313:

‘.....The organisation should select an appropriate method for identifying, analysing and evaluating risks - which might potentially cause disruptions. ISO 31000 sets out the principles of risk management and associated guidelines

Typical elements which should be included in the context of ISO 31000 (International Standard) are as follows:

- **Identification of risks.** *Identify the risks which might potentially cause disruption to the organisation’s prioritised activities and the processes, systems, information, people, assets, suppliers and other resources which support them. Such risks may come from:*
 - *Specific threats, which may be described as ‘events or actions that could at some point disrupt activities and resources (e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure)’ and*
 - *Disruptive incidents, which may arise from vulnerabilities within resources (e.g. single points of failure, inadequacies in fire protection, lack of electrical (power) resilience, inadequate staffing levels; poor IT security & resilience etc.)*
- **Evaluation of risks.** *Evaluate which disruption related risks require control / treatment. The evaluation should focus on the resources required by activities with high priority or with significant replacement lead time..... and*
- **Identification of risk controls / treatments.** *Identify treatments which can deliver the **business continuity objectives** and are in accordance with the organisation’s risk appetite (4.1)*

NOTE. If any other analysis of risk has been undertaken by the organisation or external bodies, it could provide useful information which might be of relevance to the risk assessment procedure.....’

To review the author’s (i.e. author and owner of this guideline document - the one you are now reading) thoughts on this unfortunate situation - in which ISO 22301 and ISO 22313 may have now placed many ‘amateur’ BC practitioners with regard to ‘risk assessment’ - see Note 6 / page 7 of this guideline document





Section 5 / 2B / 4

Business Continuity Requirements - Resources Analysis

The outline method of accomplishing this analysis has already been described in [Section 5 / 2A](#)

The BIA analysis will actually capture much of this data if completed correctly and, practically speaking, the two analyses might be better merged into one

Section 5 / 2B / 5

Understanding the Organisation - Summary

- Appoint most appropriate person to the task
- Re-confirm top management backing and support
- Account for stakeholders with regard to their interests in the organisation (and vice versa)
- Make all appropriate preparations for the BIA and RA
- Conduct the BIA and the RA
- Analyse and assess the BIA and RA 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'





Some External References re Section 5 / 2 - BIA and RA

For some further perspective on what has been written in Section 5 / 2 above (related to BIA / Risk Management / Assessment specifically) - appropriate sections of the documents / information found by following each of the below links might be found useful. Some is 'official' and some comes from commercial sources

Some is detailed and some provides just a simplistic overview. The user / reader will note the sad lack of *aviation specific* Business Continuity related references and, in contrast, the relative abundance of *risk* information in this area - never forgetting that pedantically speaking, Business Continuity is simply a constituent part of (overarching) Risk Management:

Business Impact Analysis

'Business Continuity Management Guidelines'

https://www.icwa.wa.gov.au/_data/assets/pdf_file/0010/6112/Business-Continuity-Management-Guidelines.pdf

Government of Western Australia - an excellent introduction to BC as related to public (government etc.) organisations. Whilst not aviation related it covers the basics very well indeed. For BIA related material see 'list of contents' at front of the above document. However, the entire document is well worth reading (Edition 3 - June 2015)

'Business Analysis - Example Template'

http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCcQFjAB&url=http%3A%2F%2Fwww.manchester.gov.uk%2Fdownload%2Fdownloads%2Fid%2F21427%2Fmbcf_business_impact_analysis_template&ei=cd7xU_gFafE0QXiv4GQAAQ&usg=AFQjCNGUJQLPmAA5OhL0EiquFH-eF9QdTA&bvm=bv.73231344,d.d2k

Local Government / Manchester (UK) / Business Continuity Forum - (January 2014)

Risk Management

'Risk Management Guidelines'

https://www.icwa.wa.gov.au/_data/assets/pdf_file/0009/6111/Risk-Management-Guidelines.pdf

Government of Western Australia - same as with its BC equivalent (see further above), an excellent introduction to Risk Management - but again, not directly aviation related. You should read the entire document (Edition 3 - Sep 2014)

Risk Management

http://www.finnairgroup.com/investors/investors_9.html

A useful, concise explanation regarding how Finnair manages its Risk Management accountabilities





British Airways

<http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCIQFjAA&url=http%3A%2F%2Fphx.corporate-ir.net%2FExternal.File%3Fitem%3DUGFyZW50SUQ9NTYzNTg2fENoaWxkSUQ9MjYzNjgxfFR5cGU9MQ%3D%3D%26t%3D1&ei=KgOhVYOFEMKS7AaLhqPgDg&usg=AFQjCNGGVEPLLcjVAd3I5pQ6AmD1UYapog&bv=m=bv.97653015,d.ZGU>

BA - 2013 Annual Report - see pages 8 and 9 - 'Principle Risks and Uncertainties'

Managing Enterprise Risks in a Global Airline

<http://www.iaaia.com/PDF/Day%20one/6.%20Neohapsis%20Kevin-George-Mark%20%2816.15-17.15%29%20Managing%20Risk%20in%20a%20Global%20Airline%20-%202010-10-10%20v0%2010.pdf>

Commercial site / possibly somewhat complex / technical in areas - but some good, useful information in between

Indianapolis Airport

<http://www.aci-na.org/static/entransit/GS7-Marsha%20Stone.pdf>

A useful 2008 PowerPoint presentation from Indianapolis International Airport - demonstrating how it uses (Enterprise) Risk Management in appropriate aspects of its everyday operations

Hong Kong International Airport

http://www.hongkongairport.com/eng/pdf/media/publication/report/11_12/E_10_Risk_Management_Report.pdf

A concise, top level report (2012) by the Airport Authority Hong Kong - concerning risk management

Business Continuity Reference Books / Documents etc. - General

Whilst we are looking at some external references the reader / user may wish to consider purchasing the following books / documents:

'Becoming Resilient - The Definitive Guide to ISO 22301 Implementation'

Can be purchased on-line (soft copy only - around USD \$40) from: <http://www.27001academy.com/> (Look under the 'BOOKS' dropdown menu)

This book provides some useful information on the 'understanding the organisation' task in general - although the connection between RA 'probabilities / likelihoods' and BIA 'impacts' should be clearer

It is not aviation related nor does it follow some of the sequences which have been described in *this* guideline document (i.e. the document you are reading now). For example, RTOs are not assigned until the 'BC Strategy' phase. It is also skewed at achieving ISO 22301 certification

The author of this book has produced a considerable degree of additional information on his website, some of it is free. In particular, there are tutorial videos and webinars - one of which (Conducting the BIA) is well worth purchasing (it is not expensive). A useful 'generic' BIA template can also be purchased





‘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

This TRB document is a useful resource for basic business continuity planning at airports. However, do note that it has been based on what is now a superseded (defunct / discontinued) standard (BS 25999) i.e. it has not been based on ISO 22301 and / or ISO 22313. However, as the latter two standards are based to a significant degree on BS 25999 - this guideline remains relevant and 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 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 \$40-45) from BCI at:

<https://www.thebci.org/training-qualifications/good-practice-guidelines.html>

DRI International - Professional Practices for Business Continuity (USA oriented)

An extract from this 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’)





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

Deliberately Blank





Section 5 / 3A - DO - DEVELOPING the BCMS / Determining BC Strategy

ISO 22313 / OPERATION / Business Continuity Strategy - 8.3

(Determining BC Strategy - **Simplified** Version [see Section 5 / 3B for full version])

What does 'Determining BC Strategy' actually mean in 'plain' language?

The information shown in this sub-section is provided in an attempt to 'simplify' the meaning, purpose and practical application of the term '*determining BC Strategy*'

This is necessary as completing this task correctly and fully is fundamental (following on directly from the preceding 'understanding the organisation' task) to the whole point of introducing BC into an organisation and, as referred to earlier in this guideline document, much of the current reference material available (including ISO 22313) is not as clear / helpful as it might be, regarding this and other, related matters

Recap

Up to this point in the BCMS implementation task we have (amongst lots of other things) identified and / or predicted an organisation's:

- BC Objectives and Policy +
- Key products / services / operations (*together with their associated key main & supporting activities and, in turn, the latter's associated processes, dependencies, 'best guess' resource requirements etc.*) +
- Risks / threats and adverse impacts (*should the risks actually occur*) to the key products / services / activities etc. +
- Target timescales (**MTPD & RTO**) within which target levels of key product / service recovery (**MBCO**) must be achieved

Consequently (and by implication), we have been able to choose (*as just one of several 'risk treatments' available*) to:

'..... **Reduce the impacts** of realised risk i.e. plan to manage / 'control / treat' the risk **after** it has actually occurred - by use of **BC measures**

The last five words above ('..... **by use of BC measures**') can simply be replaced, (with **exactly the same meaning**), with the words '**by using BC strategies**' - it's really as straightforward as that!

Note - as the choice of '**BC measures (strategies)** available' is based **initially** on a high level (strategic / big picture) view - this is why the word '**strategy**' is used in the term 'BC strategy'!





But let's pause here for a moment and have a quick look at (and comment on) how the standard (ISO 22313) introduces the subject of BC Strategy. Clause 8.3.1.1 states:

‘.....Determining business continuity strategy is about **identifying the actions** [needed to address the findings from the BIA and Risk Assessment] - in a way which **meets the business continuity objectives** of the organisation. Such action is likely to be needed before, during and after a disruptive incident.....’

So far so good (except that [pedantically] ‘actions taken **before** a potential disruptive event’ are taken as part of **risk management** and **not** as part of **business continuity**)

The clause goes on to state that ‘..... such actions * **may** for example include’:

‘.....reducing the overall impact of a disruptive incident through business continuity arrangements - which **shorten the period of interruption** and **reduce its intensity** - to acceptable levels.....’

* Note - the word ‘**may**’ as used above should obviously be replaced with the word ‘**must**’ - otherwise we have wasted our time, effort and the last 200 pages or so of this guideline document in getting to this point

The last bit of this clause which we will look at here states:

‘.....The organisation should determine appropriate strategy options for:

- Protecting prioritised activities
- Stabilising, continuing, resuming and recovering prioritised activities
- Mitigating, responding to and managing impacts

The first bullet point listed above applies directly to ‘**risk management**’ measures - and is thus beyond the scope of this guideline document - (and probably beyond the direct scope of ISO 22313 for that matter?)

The second bullet points may be simply summarised as ‘..... **by using BC measures**’

The third bullet point above relates to **both** risk management and BC measures. In this guideline document (the one you are reading now) only the BC measures are considered and, again, may thus be simply summarised as ‘..... **by using BC measures**.....’

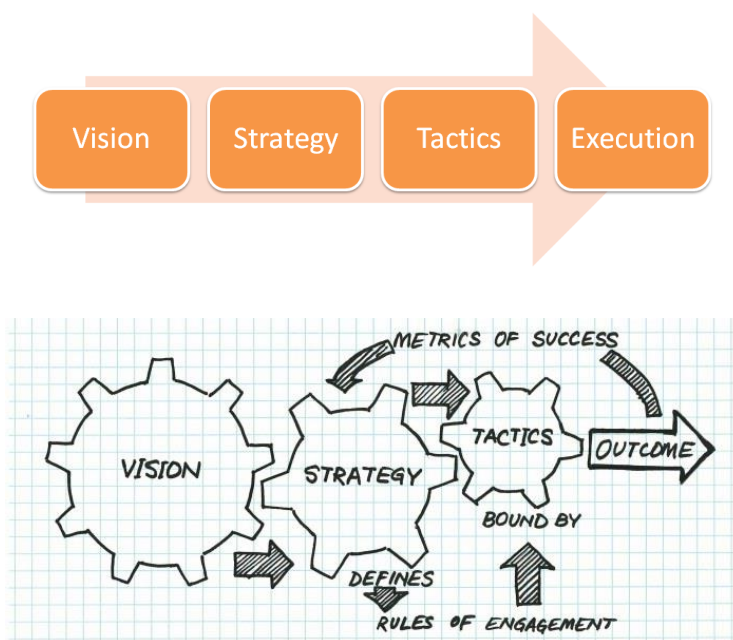
Note - use of the terms ‘**strategy options**’, ‘**options**’, ‘**measures**’ etc. - as used throughout ISO 22313 / Clause 8.3 - is somewhat confusing. Such use would appear to be made in the contexts of **both** ‘BC Strategy’ and ‘BC Tactical Treatments’ - which is the cause of the confusion

Now back to the (this) guideline document:





BC Strategy (Strategies) vs BC Tactics (Tactical Treatments) - Clarification



Strategy	- Goal (vision; desired outcomes etc.) to be accomplished
Tactic	- How to achieve that goal
Sub-tactic (Operational)	- How to 'make the tactic happen' (i.e. make it work in reality)
Outcome	- Achieved; not achieved; partially achieved?
Review (Feedback)	- Continual Improvement achieved? (Customer Satisfaction)

BC strategy provides the higher level **framework** for deciding the **actions** necessary to re-establish continuity (of product / service/operation / activity / process etc.) following a significant disruption event

Within that framework, BC tactical treatments actually **decide** and **define** those actions in sufficient detail - such that they may be further expanded upon and implemented / executed operationally - via BC **Plans & Procedures** (documentation) and by the '**BC incident response team**' (latter known in this guideline document as '**Disruption Support Units - DSU**)

Just as BIA and RA are inextricably linked - so are BC Strategy and BC Tactics (Treatments). In fact, differentiation between the latter two is almost (but not quite) academic in reality, 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





The 8 Steps of BC Strategy Implementation (Simplified Version)

We now need to **investigate** and **decide** which particular 'BC measures' (BC **strategies** + [together with] their associated, subordinate BC **tactical** treatments + [together with] the identification and co-opting / adapting / procuring / costing of all the associated **resources required** to make the strategy and treatments actually 'happen') might be suitable and appropriate to the level of adverse impact(s) - which any particular (realised) threat (risk) might pose on any particular (key product / service related) activity, process, resource etc.

This investigation & decision task / process may be simply re-worded as '**determining** (working out) **BC strategy**'

A more formal but still fairly user friendly definition of '**determining BC strategy**' goes something like:

'..... Determining BC Strategy typically involves:

- Working out which BC **strategies** will meet the BC **Policy** and other, appropriate organisational BC requirements (including [for the latter] consideration of the RTOs / MBCOs / other appropriate considerations [as they relate to specific activities, processes, resources etc.] - as obtained from the '**understanding the organisation**' task)
- Re-confirming and / or adjusting RTOs and MBCOs (as required) as a consequence of completing the bullet point step documented immediately above
- Within any particular strategy, selecting the most appropriate 'BC **tactical treatment**' responses (based on what it is [specific activity, process etc.] such responses are potentially / actually to be 'applied' to) from the available options
- Working out, consolidating, costing , budgeting and procuring the types and levels of **resources** required to meet the strategies and associated tactical treatments provisionally and / or finally chosen - as per the above

The above is accomplished as follows:

Step 1 - Choose Provisional BC Strategies

Generally speaking, there are just three choices - based on:

1. **Full, 24H** key 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





2. **Resumption of the activity**, process etc. is required - **within agreed MTPDs / RTOs** - to **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
3. **Do nothing** i.e. activities, processes etc. which (from a continuity viewpoint) can be suspended / deferred etc. The latter will be clarified in the associated RTOs e.g. 'RTO = Indefinite'; 'RTO = 6 months' etc.

Each potential BC strategy (as it relates to a specific activity, process etc.) is evaluated for advantages and disadvantages - and the most appropriate strategy tentatively chosen. Based on this choice, RTOs and MBCOs already assigned during the BIA may be confirmed and / or adjusted

In choosing the appropriate strategies, initial consideration must be given to the estimated * implementation costs (typically via a costs / benefits analysis) and also to the consequences of inaction and / or inadequate action

* Note - costs are looked at again in more detail once the provisional tactical treatments and supporting resources have been identified - see further below

Step 2 - Choose Provisional BC ('Tactical') Treatments

Having now selected a provisional BC strategy as per above (other than the 'do nothing' option) - we need to now 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 **make the selected strategy actually be able to happen / work in reality** - when needed

These latter 'specific, appropriate and adequate measures' are known in this guideline document as *** BC (tactical) 'Treatments'** - of which there is a relatively wide choice. However, the selection and use of the most appropriate BC tactical treatment 'choice / choices' (there is usually more than one) is what is important (as will be seen later)

The above tasks (selecting provisional BC strategy and associated BC tactical treatments) are repeated for every (*key product / service / operation associated*) activity, process etc. – previously identified as needing such in the BIA

* For comparison purposes, **ISO 22313** refers to '**BC tactical treatments**' variously (and confusingly?) as 'strategy options', 'options', 'measures' etc.; the **Business Continuity Institute (BCI)** calls them '*Identifying and Selecting Tactical Responses from Available Options*'or more simply '*tactical responses*'; the **USA's DRI International** knows them as '*continuity / recovery strategy options*'

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 (strategy number **3** as already referred to 'Step 1' further above) i.e. defer or suspend the specific activity, procedure etc. in question

This strategy is typically selected following a **cost / benefits analysis** of the associated BC tactical treatments available - where the potential benefits of using an appropriate treatment(s) 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 the 'do nothing' strategy it is important to identify any further potential, adverse impacts which might arise consequently **as a result of doing nothing** - and **pre**-establish appropriate counter-active measures accordingly - e.g. 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 (e.g. airline passengers prevented from flying) as a result of 'doing nothing' etc.

For another example, take an airline which needs to clear a very large backlog of passengers following a prolonged disruption event (e.g. airspace closure due to volcanic ash) - and which decides to close down its cargo operation (i.e. cargo carried in passenger aircraft) completely until the passenger backlog is cleared. Depending on circumstances 'on the day' (including the brand / reputation 'status' situation of the airline) - effective, expedient, on-going and 'meaningful' communications should be established with the cargo companies, agents, forwarders etc.

Furthermore, in situations where RTOs might be measured e.g. in months or longer, waiting (doing nothing) until after the incident is effectively over to decide on a strategy to resume / recover the associated 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 - Perform the 'Establish Resource Requirements' 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 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 confusions (e.g. that different activities, processes etc. are not being planned to concurrently use the same resource for recovery - unless feasible)
- Identifying & implementing areas of resource provision which can be consolidated e.g. where the same BC strategy & associated tactical treatment(s) might be used to meet the business continuity requirements for several different activities, processes etc.





- Looking at the opportunities for 'enabling purchasing leverage' (e.g. financial discount) when procuring the appropriate BC resources from external (third party) sources
- Validating that the BC strategies proposed are in line with the organisation's declared and current risk appetite
- Coming up with more definitive costs as related to the *entire* process of introducing a BCMS into the organisation

Important - ISO 22313 has targeted the subject of *resources* for particular attention. It is suggested, therefore, that those responsible for introducing BCMS into an organisation pay particular attention to the **RCA** (* Resources Consolidation Analysis) and other appropriate 'resources' sections of the standard - particularly if the intention is to *certify* the BCMS to BC Standard ISO 22301.....or *formally align* the BCMS with ISO 22313 . The resources addressed in ISO 22313 / clause 8.3.2 cover:

- People
- Information & Data
- Buildings / work environment - and associated utilities
- Facilities / equipment / consumables
- ICT / Technology
- Transportation / Distribution
- Finance
- Suppliers
- Partners

* See info starting page 221

Reminder: 'RCA is simply a sub-division / drill-down of 'BC Strategy'





For cross reference purposes the subject of *BC resources* also appears in:

Section 4 / 1 / 1 of this guideline - based on:

ISO 22313 / 5.2.f) - **LEADERSHIP** / Management Commitment

Section 4 / 2 of this guideline - based on:

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

Section 5 / 2 of this guideline - based on:

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

Section 5 / 3.5 of this guideline - based on:

ISO 22313 / **OPERATIONS** / BC Strategy - Establishing Resource Requirements - 8.3.2

Note - there is a significant degree of overlap in the ISO 22313 sourced clauses above. Little effort seems to have been made within ISO 22313 to better manage / mitigate such overlaps (which may be potential source of confusion to some users / readers)

Step 4 - Assess / Review BC Strategy Implementation Costs etc. - via a 'Cost / Benefit' Analysis

- Estimate cost of implementing & maintaining continuity (BC Tactical Treatments) for the chosen BC strategy / strategies (using the information from 'step 3' above - together with any other financial considerations to be accounted for)
- Validate that the BC strategies etc. proposed to be implemented are in line with the amount and / or type of business / activity etc. at risk e.g. a million dollar BC strategy is obviously inappropriate when related to protecting \$100,000 worth of associated business - whereas the same strategy might be wholly appropriate where e.g. danger of death or serious injury are considerations
- Where cost is not commensurate with benefit - a review of the associated BC tactical treatment(s) and / or parent strategy (strategies) will be necessary

Reminder: 'Review of BC Strategy Costs' is simply a sub-division / drill-down of 'BC Strategy'





Step 5 - BC related Communications with Stakeholders and Other Interested Parties

Decide 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 (the outcomes of the BIA and RA will be useful here)

Reminder: 'BC Communications' 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 (or 'critical' in any other sense)

Decide and document the organisation's sub-strategy for reviewing and dealing with BIA identified activities, procedures, resources etc. - which were not prioritised during the BIA for 'BC related action' purposes, but which were nevertheless though 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 chosen 'BC Strategies' and their 'BC Treatments' (together with estimated costings and any other appropriate information) to Top Manager for approval and 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 on the next page - we shall look at all of the above steps again, but this time in more detail - and in commonly used BC terminology (i.e. not using 'plain language')





Section 5 / 3B - DO - DEVELOPING the BCMS / Determining BC Strategy

ISO 22313 / OPERATION / Business Continuity Strategy - 8.3

(Determining BC Strategy - **Formal** Version [see Section 5 / 3A for *simplified* version])

Section 5 / 3B / 1

Cross Reference ISO 22313 - 8.3.1

Assumption

Moving forward, it is assumed that the user / reader has already 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

The underlying causes of the scenarios are irrelevant. **Some typical** scenarios for consideration (mixing & matching to the organisation's actual [real life] circumstances) **might** include:

- Safety related crisis (e.g. * catastrophic aircraft accident; unsafe ATC procedures etc.)
* As a direct consequence, the accident airline's main operating airport is closed e.g. for 2 weeks
- Security related crisis (e.g. hijack / unlawful interference, credible bomb warning etc.)
- Statutory / regulatory related crisis (e.g. major, long term regulatory breach)
- Brand / image / reputation related crisis (e.g. the top manager has been stealing money from the staff pension fund e.g. the 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
- 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)
- Staff and / or public wellbeing related crisis (e.g. terrorism or pandemic again)
- Environmental related crisis (e.g. volcanic ash)

Such scenarios will also be of use later (Sub-section 5 / 4) when preparing **BC Plans**





Reminder 1

With regard to the outputs of the ‘understanding the organisation’ task (Sub-section 5 / 2) - the organisation is now ready to determine, select, work out associated resource requirements and provisionally cost (and gain top management approval for) the most appropriate BC Strategies & their associated BC Tactical Treatments

The user / reader is reminded (see also page 204) of how ISO 22313 introduces this subject and how the latter has been ‘interpreted’ *for the purposes of this guideline document* i.e.

- Protecting Prioritised Activities (8.3.1.2)

This is essentially a ‘risk management’ responsibility (*i.e. via use of risk strategy and risk treatments / controls*) - and is mentioned here for context & information purposes only, as it is beyond the scope of this guideline (except as part of the ‘understanding the organisation’ process in sub-section 5.2)

- ‘Stabilisation, continuity, * recovery & resumption’ (8.3.1.3) are described in *this Sub-section 5 / 3B* (of the guideline document)

* The term ‘Recovery’ (see Glossary definition of ‘Business Recovery’) is mentioned in this guideline document for contextual purposes only - as the concept and practice are beyond the scope of this guideline

- Mitigation, response (to) and management of adverse impacts (8.3.1.4)

Adverse impact ‘mitigation’ measures (within the BC context *only*) are described in *this Sub-section 5 / 3B*

‘Response to and management of adverse impacts’ (within the BC context *only*) is covered in *sub-section 5 / 4* of this guideline document

Reminder 2

Use of the terms ‘strategy options’, ‘options’, ‘measures’ etc. - as used throughout ISO 22313 / (Clause 8.3) - might be somewhat confusing. Such use would appear to be made in the contexts of *both* ‘BC Strategy’ and ‘BC Tactical Treatments’, and this is the cause of the potential confusion

In contrast and in *this* guideline document (the one you are now reading) the differentiation is clear i.e. it is either ‘BC Strategy’ or ‘BC Tactical Treatments’. As already mentioned earlier, whilst the latter two terms are inextricably linked and may often be used synonymously - they are (at least pedantically speaking if not in practice) different





5 / 3B / 2 - General

*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*

Adequate completion of the tasks / requirements specified in this sub-section 5 / 3 should ensure that the determination of **BC strategy** (along with everything else which follows on as a requirement of this sub-section 5 / 3 e.g. choices of **BC Tactical Treatments**; provisional identification and costing of associated **resources**; how to deal with disruption related '**work backlogs**' etc.) within the organisation adequately supports the delivery of its key services / products / operations - via the latter's associated key 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 tactical treatments might themselves introduced new risks which, not having been considered in the 'understanding the organisation' task, would then require such consideration

Documentation of a finalised BC strategy (along with everything else which follows on etc.), + '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
- 'Embedded' in all appropriate BC documentation (especially BC plans - see sub-section 5 / 4)
- Actively referenced during all BC training and exercising

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 and production of associated BC plans & procedures) but it can also be used to keep any **actual** BC response on approximate course, despite the possibly various conflicting & confusing tactical parameters which might prevail in such circumstances 'on the day'

5 / 3B / 3 - Selecting BC Strategy

This task has already been described in Sub-section 5 / 3A, **Step 1** (starting page 206). Whilst this is an important task, it is relatively simple to perform and is not described further here except for what is written below:

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 or abandonment





Review of BC Strategy

A review of active BC strategy 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 BIA, RA etc.

A **significant change** in any of the following should also prompt review of BC strategies:

- Major change(s) to strategic business objectives
- Significant change(s) in internal business processes, location(s), technology etc.
- Significant change in the external environment, such as regulatory, market, supply chain changes etc.

An appropriate **maintenance** policy should be established to ensure that BC strategies remain accurate, current, complete and adequately documented

External Parties (Suppliers)

ISO 22313 (8.3.1.5) requires that the 'business continuity (arrangements) of suppliers' should be evaluated by the organisation (being supplied). This requirement obviously belongs in Clause 8.2 (BIA and RA) of ISO 22313 and **not** in clause 8.3 (BC Strategy)

However, sub-section 5 / 2 of this guideline has already covered the above requirement adequately as the below extract indicates:

*'.....Where such MTPDs and RTOs relate to **external** organisations - estimation and application of same will need to be negotiated and agreed with such external organisations - e.g. via contractual 'service level agreements' or similar.....'*

5 / 3 / 4 - Selecting, Implementing & Managing (**Tactical**) 'BC Treatments'

This sub-section 5 / 3 / 4 requires the investigation, selection, documentation (and eventual approval) of the appropriate **tactical** measures (**BC Tactical Treatments**) considered necessary to ensure continuity of operation (as per the associated BC strategy) during / following a significant disruption event to the organisation

The chosen BC tactical treatments 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 are chosen so that they might:

- Meet the requirements of the associated (parent) BC strategy
- Be appropriate to the organisation (size, complexity, location, methods of doing business, etc.)
- Meet declared budgetary, resources and other constraints
- Be in line with the organisation's declared and current 'risk appetite'

The generic *scope* and *choices* of BC tactical treatments are typically related, in one way or another, to (single and / or combined) uses of: [ISO 22313 - {8.3.2} refers]:

- People (including their skills, experience & knowledge)
- Information & Data (hard copy and electronic [soft copy])
- Buildings (premises), Work Environment & associated Utilities (Electricity, Water etc.)
- Facilities, Equipment (including Plant) and Consumables
- Technology (predominately ICT)
- Transportation
- Finance
- Suppliers
- Other appropriate Stakeholders / Interested Parties (not already included above)
- Emergency Services (usually provided and funded by national / local government etc.)
- Any other appropriate resources (not already included above)

The task now is to:

- Identify the *available* BC tactical treatments (falling within the scope of the associated BC strategies) as specifically appropriate to *each* designated activity, process etc. outlined in the *outcomes* of the '*understanding the organisation*' task
- Provide inputs to identifying the *costs and difficulties / complexities* associated with *resourcing, implementing & maintaining* such tactical treatments
- *Provisionally select the most appropriate BC tactical treatments* for intended actual use - and
- Confirm that the provisionally selected tactical treatments (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 *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 * **provisionally** agreed to and approved by top management
 - * 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)
- Top management agreement and approval ** **in principle** - for the funding and resource acquisition necessary to eventually implement the agreed BC tactical treatments
 - ** 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 - together with a provisional list of personnel / staff assignments for undertaking such tasks

Note 1 - it may be necessary to **re-appraise the 'parent' BC Strategy** - should the associated and most appropriate BC tactical treatment choices prove unavailable or too costly

Additionally, where the only tactical treatments available prove to be too costly, the affected product(s), service(s), operation(s), key activity (activities), associated processes etc. may be nominated instead as **exclusions** from the BCMS scope as per ISO 22313 - Clause 4.3.2

*** Lastly, where the organisation estimates that a particular threat is 'extremely unlikely' to be realised and / or the cost of protecting a prioritised key activity, procedure etc. will be prohibitively expensive, it may choose instead to **accept the risk** and re-evaluate it as part of its on-going BCMS **performance evaluation** - as per ISO 22313 - Clause 10

*** Comment from author / owner of this information document - the above paragraph is taken directly from ISO 22313 (bottom of page 21). It demonstrates again the inadequacy of this standard in some areas - in this case:

- 'Performance Evaluation' is covered in ISO 22313 - clause 9 - **not** clause 10
- What does '**accept the risk and re-evaluate it as part of its on-going BCMS performance evaluation**' actually mean? The wording is far from clear e.g. the word '**risk**' is used - so does this mean that we need to look to elements of risk management (other than the business continuity element / component) as a solution here

Furthermore, there seems to be nothing in ISO 22313's 'performance evaluation' related clause 9 - which clearly indicates how the organisation '**accepts the risk and re-evaluates it**'. With a bit of convoluted thinking it is just possible that clause 9.3 (Management Review) might be what is being referred to here - but its wording is such that it might equally not be!!!!





5 / 3 / 4 / 1 - Examples of Typical 'BC Tactical Treatments'

Generic BC tactical treatments as per [ISO 22313 8.3.1.3](#) (related to identified key activities, procedures, dependencies, supporting resources etc.) typically include - (the list is not exhaustive):

- **Activity** relocation
- **Resources** relocation and / or reallocation (including people) and / or replacement
- Establishment of **alternative processes** (+ associated procedures etc.)
- Creation of **spare capacity**
- Augmentation of **skills** (e.g. via cross-training)
- Temporary **workarounds**

See clause [8.3.1.3](#) itself for fuller details of the above

DRI International - *Operations*

Typical (Generic) BC tactical treatments for '*operations*' (the latter covering all activities other than 'technology') - according to the USA's [DRI International](#) (DRII) - include (the list is not exhaustive):

Note - the following 2 BC tactical treatment *lists* are taken from the DRII document - '*Professional Practices for BC Practitioners*' - version [1 / 2012](#)' (Reader should check for any later version) (NB: **BC tactical treatments** are (somewhat confusingly) known therein as '*continuity strategies*')

This latter document is freely available from the above website after a simple registration process

Whilst the document is obviously **USA oriented** (and this should be accounted for where appropriate) it provides a refreshing alternative to [ISO 22313](#) e.g. in areas it is much clearer, more comprehensive (and less confusing) in its explanations etc. The below is an example of this. And remember, **it's free** whereas [ISO 22313](#) costs around USD\$ 160 ([2018](#) price)

- Do nothing and repair or rebuild at time of disruption
- Develop manual workaround procedures
- Develop reciprocal agreements (more common in small business operations, the public sector and manufacturing environments [but it can also work well in the aviation context e.g. airline alliances; codeshares; mutual aid agreement etc. Same goes for airports re mutual aid agreements with organisation 'in the surrounding community'])
- Identify internal dual usage space which could be equipped specifically to support continuity (conference rooms, training rooms, cafeterias, etc.)
- * Identify an appropriate, external alternate site(s)

* When reviewing Alternate Site choices - check for acceptability of:

Location; Available space; Suitability of space(s) vs the needs of using that (those) space(s);
Communications capabilities (e.g. voice / data); Equipment available; Availability of raw materials; Hardness of site (i.e. redundancy in terms of power, water, heating / cooling etc.)





- Contract with third party service providers / outsourcers
- Transfer workload (activities) to a surviving site
- Transfer staff and workload to a surviving site
- Suspend non time-sensitive operations in a surviving site - and then transfer people / workload from the impacted site (displacement) to the surviving site
- Have staff work from home

Concerning hard copy documentation - consider:

- Photocopying / Scanning / Use Fiche / Filming (photographing)

Assess viability of continuity strategies (BC tactical treatments) against the results of business impact analysis / RTOs by:

- Comparing solutions
- Accounting for advantages
- Accounting for disadvantages
- Considering costs (start-up, maintenance & execution)
- Looking at mitigation capability and control options
- Ability to meet defined RTO and RPO

Note - BC operations related to the USA specifically - do **not** use the concept of MTPD. RTO is used instead (in the USA) to cover the **combined** meanings of MTPD and RTO (merged). For the purposes of **this** guideline document (the one you are reading now) MTPD and RTO **are** treated as separate calculations - and used as such accordingly

Develop preliminary cost / benefit analysis

DRI International - *Technology*

Typical (Generic) BC tactical treatments for '*technology*' - (according to the USA's DRI International) include (the list is not exhaustive):

- Do nothing and repair or rebuild at time of disaster
- Develop manual workaround procedures
- Implement an '**active** / **active**' (mirrored) technology environment via a manned, **dual** data centre - thus eliminating the need for continuity / recovery
- Implement an '**active** / **passive**' technology environment for **high availability** of time-sensitive technology - providing for quick restart of same
- Contract with third party service providers / outsourcers to provide a technology continuity / recovery environment. This can include:
 - ❖ A traditional '**Hot Site**' contract with a vendor - where the vendor provides the continuity / recovery equipment (to the organisation / entity) from their own inventory
 - ❖ The organisation places its own continuity / recovery equipment 'on the floor' of a vendor's data centre





- Outsource the organisation's technology environment (e.g. cloud computing etc.)
- Identify a '**Warm Site**' where continuity / recovery could occur - but only 'populate' the site with technology following an appropriate level of disruption
- Identify a '**Cold Site**' where recovery could occur - but only construct and equip the site following an appropriate level of disruption

Concerning **data** in electronic form:

- Physical and Virtual Tape backup i.e. any of:
 - ❖ Full backup
 - ❖ Incremental backup
 - ❖ Differential backup

- Asynchronous replication

Advantages compared to synchronous replication = works over longer distances; is faster; is cheaper. **Disadvantages** = possibility of some data loss if source of data [which is being replicated] fails

- Synchronous replication

Advantages compared to asynchronous replication = generally no loss of data being replicated if source of data [which is being replicated] fails). **Disadvantages** = only works effectively over relatively short distances; is slower; is much more expensive





5 / 3.5 - Establishing Resource Requirements

Cross Reference ISO 22313 - 8.3.2

Establishing Resource Requirements - General

The organisation should determine (work out) the **resources** (sourced internally and externally) which it will be required to provide in order to implement the selected BC strategies (via the latter's associated BC tactical treatments) **together with** e.g. the **eventual** production of BC plans & procedures; the setup and manning of an Incident Response Structure; the setup and operation of a training and exercise regime; conducting actual business continuity response operations etc.

The organisation should consequently develop and establish:

- The appropriate * **manpower** resources necessary to ** implement, operate, maintain, test and review the BCMS

* **Already been covered** in this guideline - see sub-section 4/2.3 - page 106

** **Over and above** those **already** assigned to the project so far

- **Robust capabilities and procedures** 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

Where necessary, the above shall include the acquisition of appropriate, external resources e.g. an alternate operating site; engagement of third party specialists and / or specialist organisations; use of an alternate workforce; arranging mutual assistance support agreements etc.

- The appropriate '**administrative**' etc. (e.g. HR; Finance; Legal etc.) **capabilities and processes / procedures** necessary to support all appropriate aspects of the BCMS. All such processes etc. shall be **prioritised** where circumstances so require - 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 avian 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 / procedures (regarding provision of BC resources) for other interested party assistance, strategic alliances, mutual aid etc.





As already documented, the generic *scope* and *choices* of BC tactical treatments (falling within associated BC strategy scope) are typically related, in one way or another, to (single and / or combined) uses of:

- People (including their skills & knowledge)
- Information & Data (hard copy and electronic [soft copy])
- Buildings (premises), Work Environment & associated Utilities (Electricity, Water etc.)
- Facilities, Equipment (including Plant) and Consumables
- Technology (predominately ICT)
- Transportation
- Finance
- Suppliers
- Other appropriate Stakeholders / Interested Parties (not already included above)
- Any other appropriate resources (not already included above)

Of course, all of the above are, in one way or another, *resources*

Concerning expansion (further explanation) of the above, *ISO 22313* - (clauses 8.3.2.1 to 8.3.2.9) should now also be consulted. Note that this ISO 22313 list finishes with 'Suppliers'

Outcomes from the above should include:

- A consolidated list (with estimated costings where appropriate) of all *internal* resources required to fully 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 required external resource(s) which are or might be unavailable (for whatever reason)
- A determination of *how to best source external resources* (e.g. consolidation, leverage [discounting] etc.)
- *Providing Top Manager with an evaluation report* of the 'establishing resource requirements' task - together with any associated recommendations, potential problems etc.
- Obtaining *agreement & approval from Top Manager for changes* (if any) to *provisionally* chosen BC tactical treatments (and possibly BC strategy), as a consequence of any of the above
- (Where necessary) - *updating projects list* for the BC tactical treatments implementation task
- *Assisting in the determination of* the structure of the Business Continuity Plan(s); establishment of the IRS etc. - which are to follow (see sub-section 5 / 4 of this guideline)

Note - the outcomes above should be considered to be provisional until such time as they are confirmed - following the appropriate cost / benefit analyses (sub-section 5 / 3 / 6 of this guideline refers)





Establishing Resource Requirements - Review

A **review** of the BCMS 'resources required' should be conducted whenever there has been a **significant change** in a BC strategy and / or BC tactical treatment(s)

A similar review should be conducted where there have been changes which potentially affect the provision of **internal** BC resources - and also when an appropriate **external** contract comes up for renewal; when the **external environment** changes significantly etc. This review may result in changes / updates to the appropriate BC strategy and / or the BC treatment(s)

An appropriate **maintenance** policy should be established to ensure that the outcomes of the 'establishing resource requirements' task remain accurate, current, complete, are adequately documented etc.

5 / 3 / 6 - Cost / Benefit Analysis

Use a 'costs / benefits' analysis to assess the **financial viability** of implementing the provisionally chosen BC strategies / treatments:

- Estimate the costs of implementing and maintaining chosen BC strategies / tactical treatments (this has probably already been accomplished via the steps already outlined further above. If not, estimated costings should be made now)
- Validate that these costs are commensurate with the 'amount' of the business / operation at risk (e.g. a million dollar BC strategy / tactical treatment may not be financially commensurate with protecting \$100,000 worth of business **BUT** - may be commensurate where the same business (operation) has significant regulatory and / or safety implications etc.)
- Where cost is not commensurate with benefit - a review of the associated BC tactical treatment(s) and / or associated BC strategy (strategies) will be necessary

Outcomes from the above should provide / include:

- A final 'chosen' BC strategies list
- A final 'chosen' BC treatments list
- A final project plan for implementing chosen BC tactical treatments
- A final consolidated list of resource requirements
- A **provisional** project plan (moving forward) for implementing BC Plans; setting up of the IRS etc.
- The **most accurate estimates available** of the costs involved in implementing and maintaining the chosen BC strategies / tactical treatments





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)

A similar review should be conducted where there have been changes which potentially affect the provision of **internal** BC resources - and also when an appropriate **external** contract comes up for renewal; when the **external environment changes** significantly etc. This review may result in changes to the appropriate BC strategy and / or the associated BC tactical treatment(s)

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 / 3.7 - Final Agreement & Approval

The desired outcomes are:

- Top Manager (TM) agreement to and approval of the recommended BC strategies and associated BC tactical treatments
- TM agreement to and approval of the implementation, co-opting and procurement tasks related to the recommended BCMS resources requirements (including agreement to and approval of the estimated costs / budget)
- TM agreement to and approval of the implementation (project) plan associated with **the above**
- **Moving forward** from this BC Strategy phase, TM agreement to and approval of the provisional BCMS **implementation** (project) plan

BC Tactical Treatments - Review

A **review** of 'in-force / active' BC tactical treatments should be carried out at least every 12 months - and / or following any change to the associated parent BC strategy. Any **significant** changes in 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 in some significant way to the activities, processes etc. (e.g. legal and regulatory)

An appropriate **maintenance** policy should be established to ensure that active BC tactical treatments remain accurate, current, complete and adequately documented





5 / 3 / 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 will need to 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.). All types / formats of communication should be considered e.g. written (both hard and soft copy); spoken (verbal press releases; press conference); social media and similar etc.

In particular, careful pre-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) plan in place (see Glossary), it is more than likely that the 'requirement to communicate during crisis' has *already* been planned for (typically as part of an overarching *crisis communications strategy* as mentioned above) and, if so, can be easily adapted to BC purposes

5 / 3 / 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

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 usual methods of 'catch-up' are

- 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





5 / 3.10 - Dealing with Activities, Processes etc. **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 the BC Strategy

It is now appropriate to **review this list again** to see if this 'status' (of all the included activities etc.) 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 trigger such a review. A convenient time for annual reviews would be at the same time as the BIA review, if possible

Should a review identify that an activity, procedure etc. **does** subsequently require inclusion under BC Strategy - then action should be taken accordingly e.g. assign MTPD, RTO and MBCO. Include as part of the appropriate BC strategy. Assign appropriate BC tactical treatments. Ensure associated resources are provided. Include in the BC Plan etc. Should a significant cost be involved then firstly seek approval to proceed from TM





A 'real life' example of a 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 of an ***aviation*** related BC Strategy

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 [10](#) of this document

All contributions will be gratefully received and the source acknowledged herein





Deliberately Blank





Section 5 / 4 - DO - DEVELOPING and IMPLEMENTING the BCMS

The Incident Response Structure + BC Plans & Procedures

ISO 22313 / OPERATION / Establish & Implement BC Procedures - 8.4

Despite the *misleading* ISO 22313 title 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

* Note - see again Glossary section at the front of this document (pages 33 to 34 and 'IMPORTANT NOTE' - pages 62 to 63) to refresh on understanding of the use and context / relationship of the words '*incident*', '*crisis*', '*emergency*', '*contingency*', '*incident response structure*' etc. - as used above + their relationship with the *concept of a business continuity plan* / structure / system

** Otherwise known in this guideline document *only* as '*Disruption Support Units* - DSU'

INCIDENT RESPONSE STRUCTURE (IRS)

ISO 22313 - 8.4.2

The Emergency Response Team

Disruption is inevitable in some form, at some time to any organisation. BUT..... the first response priority of the organisation might typically *not be* a business continuity matter at all - but instead might relate to responding to the *immediate* consequences of the disruption itself, particularly where such consequences relate to a major emergency / crisis type situation in circumstances where danger of death *and / or* serious injury *and / or* major loss of property / facilities *and / or* significant financial loss *and / or* serious adverse impact on reputation etc. - are possible

Aviation Context

A direct and almost inevitable *side effect* of e.g. a serious aircraft accident at the accident airline's major hub airport - will be significant disruption to the accident airline's network operations

Such disruption typically arises as a result of e.g. closure of the airport itself (for several weeks 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' etc.





However, before this airline (and the 'accident airport' too, of course - assuming 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 its BC plan** (assuming that it has one?) **it obviously needs to respond to the immediate and shorter term consequences of the accident itself** - many of which will involve emergency response, humanitarian and welfare considerations

Note - in the paragraph immediately above we are referring to the **airline's** immediate and shorter term response and **not** to the response of the emergency services (fire and rescue; police; ambulance / medical etc.)

When pre-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 entitled the (name of airline) '**Emergency Response Team (ERT)**'

Similar arrangements (typically with different, 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 the aviation context)

As the nature of the disruption associated with the aircraft accident referred to above (we shall be using this same example throughout this sub-section) becomes apparent, the airline's (separate) '**Business Continuity Team**' (BCT) will probably also be activated (typically by the person in charge of the **ERT**) and 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 the aviation context)

As the effects of the disruption begin to lessen it will be time to start converting business continuity operations back to their 'normal operations' status. This process is known 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

So far we 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 (IRS) as described above (or similar) has **not** been put in place, the best that could generally be managed by any organisation (when 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 methods of response - which 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 233
- 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 conducts both emergency and BC operations and shares C4 resources





- For the smallest organisations, the roles and responsibilities of the 4 teams documented above might need to be typically assigned to just e.g. two or three persons! This is a far from ideal situation - but there may be little or no choice in the matter. The 'one person' team should be avoided if at all possible - for obvious reasons (single point of failure)
- In many organisations (especially where manpower resources are limited) *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) 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 this 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

Other than this, this method of *C4* does not 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 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 best avoided)

Such volunteers should be treated with consideration and respect - and top management should regularly recognise their contribution in one way or another e.g. as part of any 'recognition and reward' scheme - if available

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. free food, beverage and entertainment) annual parties for all volunteers





A Typical Incident Response Structure

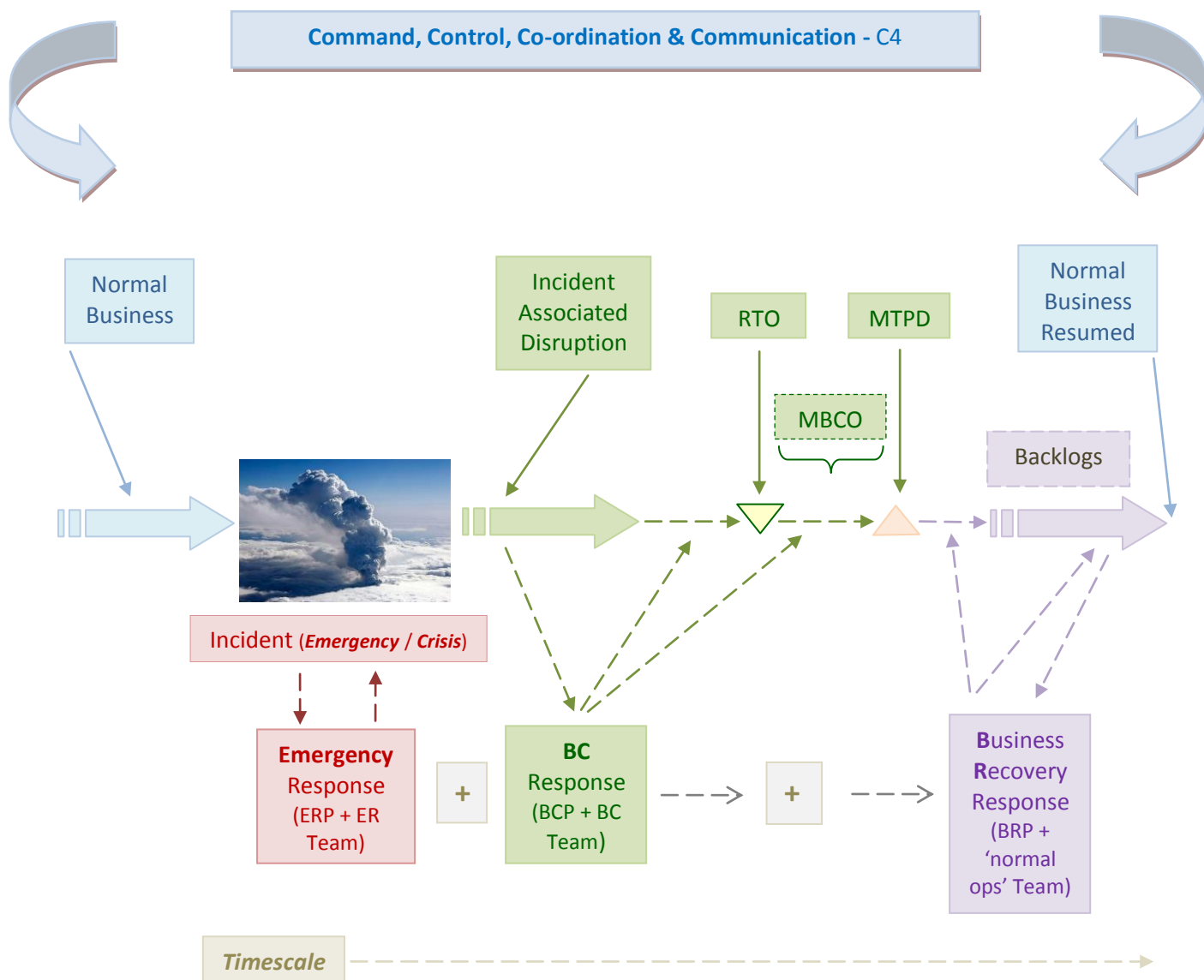


Fig 22 - Typical IRS - Depending on nature of incident, timescale can run from minutes to hours; from hours to days; from days to weeks and, in extremis, from weeks to months or even longer. Time overlaps of **ER**, **BC** and **BR** operational functions is to be expected

- **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; 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 backlogs; resume normal service levels etc.





Levels of Command, Control, Co-ordination & Communication (C4)

C4 systems operate in general at three levels of responsibility and accountability - i.e. strategic (top level), tactical (intermediate level) and sub-tactical /operational (lower levels)

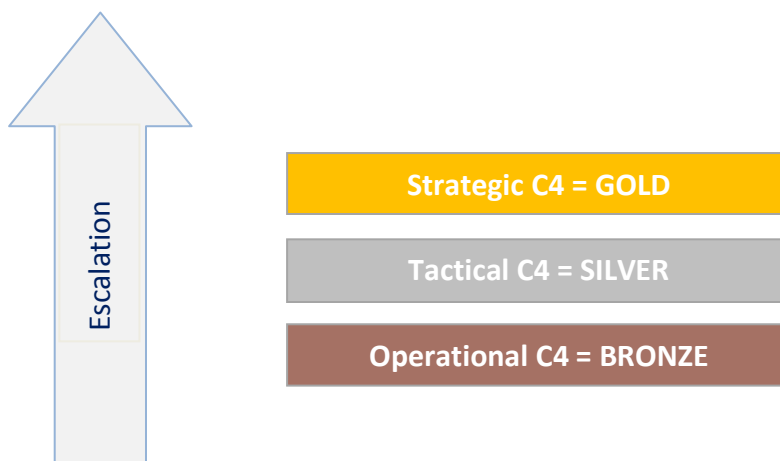
For *airline emergency / crisis response operations*, strategic C4 is typically exercised by top management; strategic to tactical C4 by a higher to middle level management group and operational C4 by lower management and non-management staff

Similar typically applies to *airport* and *ground handling agent* operations. The concept is equally applicable to business continuity and business recovery 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

For example - in the USA this 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, UAE, Oman and a small number of other countries, the C4 system is colour coded and entitled as shown below:





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 rapidly alerting and activated. Consequently, some form of 'guarantee' is therefore 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 the vast majority of airlines & airports and particularly to those which operate 24H)

This latter entails a *limited* degree of '24H on-call' capability for *designated* key team members - and this can be accomplished in a number of ways (which are beyond the scope of this guideline - and are thus not covered, except for contextual and information purposes)

Many airlines and airports use their 'operations control (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' 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 usually a degree of urgent immediacy in alerting and activating the **ERT**, the **BCT** is typically alerted and activated at some later stage (perhaps hours or even days later) - depending on the estimate of when any associated disruption will begin to adversely affect key operations. 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 persons in just a few minutes. Such systems are, in the main, supplied by commercial entities

Note - other than what has been written above, alerting and activation methodology in detail is *beyond the scope* of this guideline document

It is strongly recommended that the user / reader studies [ISO 22313 / clause 8.4.3](#) - 'Warning & Communication' - for more information on this subject





'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 diagram below)

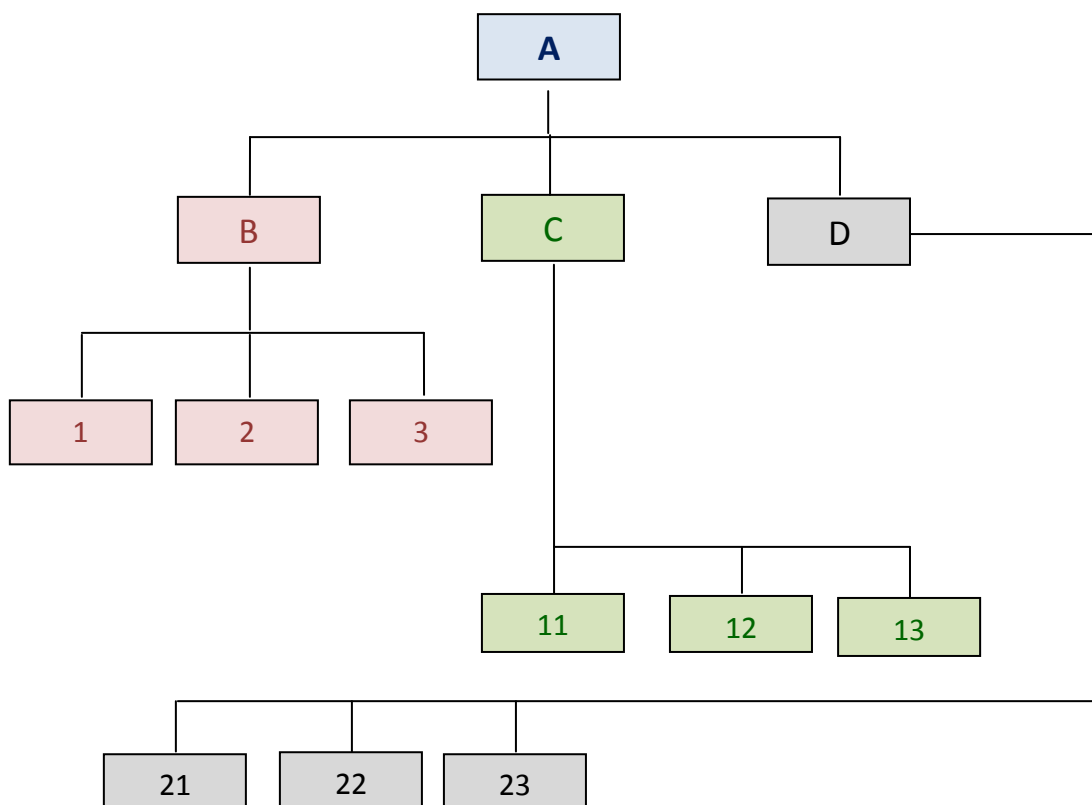
Person **C** would pass on the alerting message to a different group of persons than those contacted by person **B** - say persons **11, 12, 13, 14**, etc. and so on - until the full list of persons to be alerted has been contacted

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 takes time - especially for large numbers of persons to be contacted - and requires personal contact details (office, home and mobile telephone numbers etc.) and the associated procedures to be constantly maintained

Fig 21





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:

- Classify the incident situation's scale / severity e.g. **RED** (high severity) Alert; **ORANGE** (medium severity) Alert; **GREEN** (low severity) Alert etc.
- Initiate the 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 situational 'Big Picture'
- Keep the situational Big Picture current or as 'near current' as possible
- Ensure that those needing to acquire and retain the Big Picture (decision makers) do so
- Assess (and continually re-assess) the Big Picture situation
- Make appropriate decisions and issue to those designated to execute them
- Monitor progress of execution of the decisions referred to immediately above
- Escalate issues where deemed necessary
- Communicate - both internally (within the organisation) and externally (particularly with the 'authorities' and the 'media')
- 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 logs)
- Decide when to stand down the IRS
- Compile 'lessons learned' and ensure that action points are dealt with expeditiously and adequately

Note - The military, emergency services etc. routinely operate to a C4 structure - where generally one is either directed in what to do - or one directs others in what needs to be done. Organisations more familiar with managing 'anything' via **debate** and **consensus** might be at serious disadvantage if trying to apply this latter management style to an IRS. Training and exercising in the 'military style' method of IRS C4 management will go some way to overcoming this potential limitation. (NB: military style C4 does **not** mean that there need be a lack of initiative or flexibility - far from it. 'In the right hands' - effective and efficient military style C4 easily manages to combine both requirements)

IRS - Resources

IRS related resources should have been planned for, documented, 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





BC PLANS & associated PROCEDURES

ISO 22313 - 8.4.1

The organisation should put in place and document (in a plan) those procedures which provide overall control of the response to a disruptive incident and resume activities within their recovery time objectives. These business continuity procedures should establish the appropriate internal and external communications protocol and be:

- **Specific** - with regard to the immediate steps that should be taken during a disruption
- **Flexible** - so that they may be used to respond to unanticipated threat scenarios and changing internal and external conditions
- **Focused** - so that they may clearly relate to the impact of events that could potentially disrupt operations - and be developed based on stated assumptions and an analysis of interdependencies
- **Effective** - in terms of minimising the consequences of disruption through implementation of appropriate mitigation strategies

THE EMERGENCY RESPONSE PLAN (ERP)

As already mentioned, the **ERP** (which is *not* a BC Plan) is used (where appropriate) to respond to the immediate and shorter term consequences of the *cause* of the disruption *and not to the associated / consequent business continuity / business recovery problems*. It is implicit that this plan is only invoked in response to a major crisis - almost always where some element of 'danger to life' (or similar severity impact) is / was a factor

Reminder - the **ERP** is mentioned in this guideline document 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 'procedures, processes etc' are also included

There are various ways of writing **BCPs** - the choice being dictated by the business, size and complexity of the organisation. As our 'role model organisation' for this guideline document is a 'generic' medium to large sized entity with relatively complex issues involved - a proposed suitable guide follows below - for how a BCP for said organisation might be produced





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 top management - the 'authorities' contained in it are binding on any individual business units (**IBU**) required to participate in the organisation's BCP (appropriate [very brief] details of such IBUs also being 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**' responsibilities assigned to them. Before this can be accomplished appropriate training shall be delivered to designated IBU staff. The latter shall also periodically exercise their own BCPs - individually and in conjunction with larger scale 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, BC Policy (including 'scope') and BC Strategy 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

The Master BCP will generally 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

It is also appropriate that this strategic document contains brief details of any higher level response plans associated with disruption e.g. the internal and external communications plans designed to protect brand, image and reputation and to communicate with stakeholders / other interested parties - together with higher level direction & policy on e.g. BCP training, exercising, maintenance, monitoring, improving and reviewing

Individual Business Unit (Disruption Support Unit - **DSU**) BCPs

Note - the terms '**individual business unit**' and '**disruption support unit**' may be regarded as synonymous / interchangeable when used in this guideline document

See pages 107 to 111 - The '**Workers**' etc. - for a reminder re '**disruption support units - DSUs**'

It is essential that **each** IBU / DSU **has its own, individual BCP, specific to its own, specific BC accountabilities & responsibilities**, 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, 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' BCP than the specialist and expert DSU, most appropriately related to the particular BC tactical treatment (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 CSUs) should formulate tactical BC procedures for how it will maintain the organisation's website(s) and social media capabilities - under extremely heavy load (hits) related to a major emergency / crisis impacting on the organisation
- 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' considerations where appropriate) should access to the normal work location be denied
- For an **airline** context:
 - The airline's **Operations Control Centre's** DSU BCP should for example:
 - Include procedures for maintaining the continuity of flight operations in general
 - Include procedures for invoking (alerting & activating) the organisation's BC response
 - Manage the entire BC response until such time as the BCT can take over this responsibility
 - The '**crewing section**' DSU should e.g. have suitable BC plans for continuing to provide operating crew
 - The **aircraft engineering** DSU should take appropriate measures to ensure that aircraft servicing and maintenance operations can resume / continue
 - The **reservations offices, call centres and ticket shops / desks** should e.g. have tactical BC plans in place to deal with vastly increased enquiries from the public (*e.g. following a catastrophic aircraft accident, an airline's call centre(s) will be swamped with calls for information - and probably also to cancel flights*)





- **For an airport context** - many (airport) DSUs 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 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 the plan (A small plan is of no use if it excludes essential and highly desirable information. Conversely, no one will read an oversized plan unless most of its content is relevant to the reader)
- BCPs can be in both hard copy **and** soft copy format if desired. As an absolute basic minimum, hard copy is always preferred. At least two **hard** copies of **each** DSU BCP must be stored in a reasonably & relatively quickly accessible and secure 'off-site' location

Soft copy DSU BCPs must be available via backup systems / applications / networks which can be accessed **separately and remotely** from the primary method 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'. As a second choice the organisation's intranet (if any) can be used provided appropriate personal information / data is first removed and that a separate, secure and robust backup data source is available

- 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 / IBU) ensures that the plan is 'suitable (fit) for purpose' in all respects
- DSU BCPs shall be controlled documents (version control, contents list, list of effective pages, revision procedure etc.)
- DSU BCPs containing 'sensitive' information must be suitably protected / safeguarded
- DSU BCPs should be considered to be subordinate documents of the overarching main (**master**) BCP





Typical (DSU) BCP Contents (*this list is not 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 adequate and approved respectively
- ✓ The usual 'controlled document' requirements e.g. glossary, revision procedure, contents page etc.
- ✓ Purpose & Scope
- ✓ Objectives and associated measures of success (particularly regarding the appropriate BC tactical treatments 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 and supporting issues (e.g. resources) for which a particular DSU has been assigned business continuity responsibilities (tactical treatments 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 and supporting issue listed immediately above - BC procedures are to be documented, describing **in detail** how the specific DSU will maintain continuity i.e. how it will resource, apply, manage, monitor, measure & review its assigned BC tactical treatments (see also 'Objectives' further above in this list)
- ✓ For each BC tactical treatment 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. 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. - especially concerning crisis communications (internal and external) - as appropriate





- ✓ How information flows (in and out) are to be managed
- ✓ Communications requirements and procedures
- ✓ A comprehensive, current, indexed & otherwise well maintained telephone (& other contacts) directory, prepared specifically for use in such operations e.g. it should contain details of **all** key business unit staff, senior managers, other key stakeholders including external suppliers and customers, the emergency services, regulators, other interested parties 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 conducting continuity operations, where the use of the primary facility is denied - and also for separate and safe storage of vital, supporting resources - as appropriate

Include '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) 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 with 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.
- ✓ An easily managed list of cross-references

DSU BC Plans - Production / Implementation

After appointment of a DSU's BCP owner and (separate) approver - the DSU BCP shall be produced (by its 'owner') - following appropriate procedures and guidelines provided by the organisation's BC manager (or equivalent person)

The BCP **master** document is generally used for primary guidance in this task (e.g. it should ideally include / cross refer to comprehensive templates) - and the person who manages the master document (e.g. the organisation's BC manager or equivalent person again) should also provide all requisite 'one on one' personal support and guidance - as required by individual DSU BCP 'owners'





When the first draft of the DSU BCP is ready it should be fully reviewed (together with feedback) by firstly the 'approver' **and** subsequently the organisation's BC manager or equivalent person

Following the incorporation of (feedback provided / required) actions by the DSU BCP owner - the updated DSU Plan is distributed within the DSU and also amongst all other **appropriate** stakeholders / interested parties - for consultation and review

Further feedback is then gathered, the plan updated again where necessary, 'approved' (again) by the approver 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, improving and reviewing

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 - it is only necessary to produce DSU BC plans and procedures which cover response to specific disruptions as provided for in the organisation's BC strategy. However, a BC plan meant to deal with one particular area of disruption e.g. IT; natural disaster; facility fire etc. - is more than likely able to be 'adapted' to other (unplanned for) disruptions, of a similar nature - and this should be implemented accordingly where circumstances so require

Note - it is recommended that the user / reader also studies **ISO 22313** - clause **8.4.4.1**





Cross Reference - ISO 22313 / **Procedures - 8.4.4.3**

ISO 22313 specifically refers to certain procedures (see clause 8.4.4.3) - presumably with the intent (although this is not explicitly stated) that same should be included in **BCPs**?

These procedures (by clause number & title) are:

- 8.4.4.3.1 - Incident / Strategic Management Procedures
- 8.4.4.3.2 - Communications Procedures
- 8.4.4.3.3 - Safety & Welfare Procedures
- 8.4.4.3.4 - Salvage & Security Procedures
- 8.4.4.3.5 - Resumption of Activity Procedures
- 8.4.4.3.6 - Procedures for recovery of ICT Systems

The requirements of clause 8.4.4.3.5 have s already been covered in this guideline document. All other clauses are **outside the scope** of same - as declared further below

However, (separate) study of the above clauses is still recommended - where the user / reader considers that such a course of action might be appropriate to his / her own specific circumstances

*Scope of ISO 22313- clause 8.4.4.3 - with regard to **this** Guideline Document*

The subject of **emergency / crisis (incident) 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 **salvage & security procedures** is **beyond the scope** of this guideline document

The subject of **recovery of ICT systems** is **beyond the scope** of this guideline document





THE BUSINESS RECOVERY PLAN (BRP) Cross Reference - ISO 22313 / **Recovery** - 8.4.5

Note - The subject of Business **Recovery** (in contrast to Business Continuity) is generally **beyond the scope** of this guideline document. Accordingly, the below is provided for contextual & information purposes only (See **ISO 22313** - clause **8.4.5** for more information on this subject)

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 stood down

From this point on it is more than likely that '**normal management**' type techniques (together with the associated normal business resources and routines available to the organisation) will permit adequate return (recovery) to normal levels of business. Note that this includes the use of some / all resources which were originally assigned to the **emergency / crisis** response and / or the **BC response** - including manpower

However, and to put 'business recovery' in some context here, the recovery time can range from very quick (e.g. minutes, hours or days in the case of restoring IT type disruption) - to many months or even longer (e.g. complete demolition and rebuilding of a major facility such as a large building)

In extremis, the business recovery measures envisaged in clause 8.4.5 (see sub-paras 'a' through 'n') may need to be invoked. However, how these can be 'planned for' in advance is difficult to foresee as 'what it is that needs to be planned for' will not be known until **after** the disruption event has occurred

To quote clause 8.4.5 '*.....A decision on how best to 'return to normal' will need to be taken based 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 needed for recovery.....*'

Whilst the above is sound common sense, it is **not** a plan or even a process or procedure. And does one really require pre incident 'documented procedures' in order to assess the situation and then decide 'what to do' - **even if one could see into the future!**





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 'maintenance' are:

- 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 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 maintained. Accordingly, the BCP (or some other appropriate, associated document) must include appropriate procedures to:

1. Devise a 'system' which will identify relevant changes effectively, efficiently and expediently
2. Notify the changes to those 'who need to know'
3. Action the changes (whatever type of action is required)
4. Receive confirmation that change(s) has / have been effectively accounted for reported as such by all concerned
5. Update appropriate documentation / data
6. Where the circumstances of a 'change so requires, implement an associated training and / or information programme
7. Audit the change process

Where changes are significant, it might be necessary to go through the 'understanding the organisation' task and similar processes again - and to further update the appropriate parts of the BCP if required - as based on the results





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

Deliberately Blank





Section 5 / 5 - DO - DEVELOPING and IMPLEMENTING the BCMS

Exercising the BCMS

ISO 22313 / OPERATION / Exercising & Testing - 8.5

Note - the words 'exercise / exercising' & 'test / testing' (as used in this sub-section) may be regarded as 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 *persons* involved in BCMS - in order that they are exposed to their BC roles and responsibilities 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 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 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 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 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 the associated pre-exercise refresher training (the latter being provided in the month before scheduled exercise date)
- All appropriate feedback from previous exercises should have been responded to and the appropriate areas of concern rectified - at least 1 month before scheduled exercise date
- Appropriate initial and / or refresher BCMS training takes place in 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
- A comprehensive 'master' exercise plan is produced and generally followed to get the most out of the exercise i.e. to achieve exercise objectives
- Adequate exercise objectives should be set and changed regularly to ensure that over a series of exercises (as part of an on-going process) the whole of the BCMS is exercised (Note - for medium to large sized organisations it is unlikely [and even *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 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





Whatever is decided, a suitable exercise programme should be approved and published - typically at least one year in advance of scheduled exercise dates

A significant change in the organisation may trigger the scheduling of an exercise in order to validate any significantly revised BC arrangements

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 also cause a withdrawal of goodwill amongst volunteers (from the organisation) involved in BC planning and response

The degree of pre-planning for a **major** exercise related to a **large and complex** organisation should not be underestimated - typically requiring 6 to 12 months of planning, acquisition of supporting resources, provision of an adequate budget etc.

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 possible solution to the above problem would 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 exercise scenario and objectives every 12 months)

The exercise programme should consider the roles of all parties, including key third party providers, suppliers and others who would be expected to participate in continuity activities. An organisation may include such parties in its exercises and may participate in **their** exercises

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 - usually termed 'umpires'. Not only can they assist in the successful execution of the exercise but their critical feedback post exercise can be invaluable

Consideration should be given to inviting appropriate stakeholders / other interested parties to 'observe' exercises - typically 2 to 5 observers per exercise, circumstances permitting

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 both types of feedback should be co-ordinated, consolidated and collated (usually by the organisation's BC Manager or equivalent person) and, where required - remedial action points, corrective action allocations (to appropriate persons) and 'completion' timescales produced. This 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 to be carried out by those so assigned in the report

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 - a BCMS will be worthless unless it is adequately trained and exercised on a regular basis

Note - the detailed plans, procedures and processes necessary to conduct BCMS related exercises are (with the exception of what has been documented above) *beyond the scope* of this guideline

It is strongly recommended that the user / reader studies all of ISO 22313, clause 8.5 - with particular emphasis on clause **8.5.3**





Deliberately Blank





Sub-section 6 / 1

Check & Act

BCMS Performance Evaluation

Cross Reference - ISO 22313 / Performance Evaluation - 9

ISO 22313 *Clause 9* should be read in conjunction with the information provided in *this* Sub-section 6 / 1

- 9.1 Monitoring, Measurement, Analysis & Evaluation
- 9.2 Internal Audit
- 9.3 Management Review

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 [see BC Policy])
- Adequacy of the BCMS (i.e. that the BCMS is 'fit for purpose')
- Continual improvement of BCMS effectiveness
- Continual improvement to BCMS customer satisfaction

..... the organisation's BC Manager (or otherwise the most appropriate person e.g. the compliance / audit manager) shall plan, document, implement, maintain and review (or arrange review) the associated and appropriate **monitoring, measurement, analysis & evaluation processes** and **procedures** required to ensure and demonstrate the said 'conformity', 'adequacy' and 'continual improvement' requirements. Such processes / procedures should be applied on a regular, systematic and on-going basis

Procedures etc. for Monitoring, Measurement, Analysis & Evaluation (ISO 22313 clause 9.1)

The above procedures should adequately account for:

- Setting of **performance indicators** (including qualitative and / or quantitative **measurements**) appropriate to the needs of the organisation

Note - performance indicators should be designed so as to measure conformities and improvements to both the BCMS and its outcomes. Performance indicators may be based on any / all of management, operational and economic parameters - and should also provide the information necessary to identify both success and those areas requiring correction and / or improvement

- **Monitoring** the extent to which the organisation's business continuity policy, objectives and targets are being met





- **Evaluating** the performance of the BC measures which have been put in place to ensure the continuity of key products, services, operations, activities, processes etc.
- Proactive measures to **monitor** 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 and results of monitoring and measurement** sufficient to facilitate subsequent **corrective action analysis**
- **Providing, retaining and maintaining** associated **reports, records and other required documentation**

Use of the word '**evaluation**' in the wider BC sense typically applies to the concept of:

Customer Satisfaction (Continual Improvement - see also [sub-section 6 / 2 of this guideline](#))

Note - BCMS 'customers' are defined in this guideline as those stakeholders having some interest(s) of 'value' in the organisation. The value may be tangible or intangible. Some examples of BCMS customers typically include:

- Organisation's staff / employees
- Recipients of organisation's key product(s), service(s), operation(s)
- Shareholders
- Suppliers
- Dependencies
- Regulators

Customer satisfaction (as related to BC matters) will usually be **evaluated** via feedback provided at the end of appropriate BCMS desktop and practical (simulation) exercises, to which 'appropriate customers' have been invited (most likely as an observer but also possibly as a participant). The same applies to any **actual** BC operations (as opposed to 'exercises')

Training course critiques and similar also form a medium for **measuring** customer satisfaction - where appropriate

Appropriate records of 'customer satisfaction' reports shall be maintained

Concerning airlines, airports etc. probably the most important 'customer' of all is the potential or actual traveller (i.e. **passengers**). Obviously it is not possible to invite such customers to observe and provide feedback on BC exercises. On the other hand, they will typically be direct recipients of the adverse impacts of any **real** (significant) disruption events 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 flight (typically by 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 passengers in some 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 document

* 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 to 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 shall also strive for **continual improvement** of its products, services and operations by demonstrating compliance with its own BC Policy and Objectives (amongst other things) - and by use of audit, data analysis and management review

Evaluation of BC Procedures

See ISO 22313 - clause 9.1.2

Internal Audit (ISO 22313 clause 9.2)

Note 1 - The detailed methodologies of auditing are generally **beyond the scope** of this guideline. However, some basic explanatory material is necessary and has been included below. The user / reader should also refer to ISO 22313 - clause 9.2

Note 2 - The various types of audit (& similar) referred to below come under the general ISO 22313 heading 'Evaluations' (To quote from clause 9.1.2 '.....evaluations may take the form of **internal and / or external audits, or self-assessments**.....')

Note 3 - 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 in detail by ISO 22313

Note 4 - 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.

In principle, **internal** audits of the BCMS should be performed by the organisation's compliance / audit business unit 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 within the required timescale and to the required degree / level





A BCMS internal audit generally involves an impartial review of same, evaluated against pre-defined standards and / or policies - together with the provision of remedial recommendations (corrective action) where appropriate. Such audit should be 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 etc.

The pre-audit Process (i.e. not the audit itself)

All concerned should clearly understand (beforehand) the particular type of pre-audit processes to be used for the specific audit to be undertaken - and should follow same **prior to** an actual audit taking place. To take a typical 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) well before the audit is due

The GAP analysis provides opportunities to identify any actual or potential deficiencies (**non-conformities**) and for the organisation (or appropriate part[s] of the organisation) to take appropriate remedial action i.e. **before** the audit actually takes place

BCMS Audit (i.e. the actual audit itself)

The BCMS audit typically covers / includes:

- 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 ISOs 22301 / 22313); in accordance with a regulatory 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; 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 etc.
- Compiling & collating audit documentation and similar e.g. results of questionnaires; reports of 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. Discussing & debriefing both with appropriate stakeholders / other interested parties - and documenting the feedback
- 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 indicate if unresolved 'differences of opinion' remain between auditor & auditee
- Providing an agreed *remedial action plan* to address the agreed recommendations of the audit
- Providing a suitable *monitoring* process to ensure compliance with the agreed remedial action plan

Internal & Other Audit Procedure

Detailed internal & other audit procedures are described in (Note - this particular subject is beyond the scope of this guideline document)

External Audit

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 the very briefest of mentions in ISO 22313. Nevertheless, it is an important subject which must be adequately addressed by the organisation - where appropriate. As a reminder, the subject of 'audit' (in general) is beyond the scope of this guideline





More general Information on Audits

Audit Nonconformities

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' (top 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 are taken in response to audit / inspection / operational evaluation findings and feedback. Such procedures shall also 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 action taken has re-established compliance with the relevant requirement

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 *

* These items are the responsibility of the relevant 'Responsible Manager' - in conjunction with the auditor

Personnel Assurance Programme

Personnel 'required to manage and / or operate' the BCMS should be subject to an '**assurance programme**'. Such programme should typically:

- Define personnel 'terms of reference', accountabilities, roles & responsibilities, authorities etc.





- Define personnel Key Performance Indicators e.g. objectives, standards to be met, measurement methods to use etc.
- Define factors related to the above which determine 'success'
- Include associated Key Performance Indicators 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 appropriate records and reports, including **monitoring and measurement** data, which can be **analysed** to demonstrate the suitability and effectiveness of the organisation's BCMS

Such records and reports shall also 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 and retention rates of disruption related volunteers (e.g. those providing humanitarian / welfare services as part of the IRS)

Audit feedback should also be analysed in order to establish trends, problem areas, areas exhibiting continual improvement etc. The results shall be considered at 'Management Review' meetings

Corrective / Preventive Action - (See Sub-section 6 / 2 of this guideline document)

Review of the BCMS

General

In order to remain effective, efficient and 'fit for purpose' a BCMS should be **reviewed** at planned intervals as specified in BC Policy and also at times of significant change to the way an 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 the BCMS - typically performed by the organisation's BC Manager or 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

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 top management 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

Management Review (ISO 22301 clause 9.3)

Regular 'Management' reviews of the BCMS (independent of other reviews) will enable top management to address need for changes to key BCMS elements, including:

- Policy, objectives and targets
- Resource allocations
- Risk acceptance / appetite
- BC Strategies & associated BC Tactical Treatments

Note - the user / reader should also refer to ISO 22313 - clause 9.3





Sub-section 6 / 2

Check & Act

Continual Improvement of the BCMS

Cross Reference - ISO 22313 / Improvement - 10

Nonconformity and Corrective Action ISO 22313 - Clause 10.1

Note - The detailed methodologies of 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

Corrective and / or Preventive Action

The findings of audits, feedback reports etc. typically identify at least some 'nonconformities'

If this is indeed the situation, then preparation and implementation of timely *corrective* and / or *preventive* actions (which are *respectively* designed to correct **1**) - any *existing* nonconformities found and deal with their consequences and **2**) - to identify and prevent *potential* nonconformities before they can occur) is necessary. A third categorisation is also often made - and is generally known as an '*observation*'

In most aviation related organisations the subject of 'nonconformity and corrective action' is not managed (apart from self-assessment / operational evaluation) by anyone who is part of or closely related to the organisation's BC business unit. (The organisation's *compliance / audit* business unit [or equivalent] typically assumes this responsibility)

Corrective Action - is taken to eliminate the cause of identified, *actual* deficiencies (non-conformities) in order to prevent re- occurrence. Top management should ensure that corrective actions are implemented and that there is systematic follow-up to evaluate the effectiveness of such actions. A typical process comprises:

- Identify nonconformities
- Determine root cause(s) of nonconformities
- Evaluate various remedial action plans for removing nonconformities
- Choose and implement the most appropriate remedial action plan(s) - otherwise known as 'corrective action(s)'
- Document all of the above
- Review (monitor) any corrective actions taken





Preventive Action - is taken to eliminate the cause(s) of identified, **potential** deficiencies **before** they can occur. A typical process comprises:

- Identify **potential** nonconformities
- Determine cause(s) of potential nonconformities
- Evaluate various remedial action plan(s) to remove potential nonconformities
- 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

IMPORTANT

See 'note' to [Section 4 / 1.6](#) (page [93](#)) of this guideline document re further explanation re meaning / interpretation of the term '**preventive action**'

Observation - An item of objective evidence found during an audit. An observations is **not** a nonconformity

Continual Improvement ISO 22313 - Clause 10.2

In the context of continual improvement, the organisation may acquire knowledge on new BCM technology and practices, including new tools and techniques. These should be evaluated to establish their potential benefit to the organisation

See also 'Customer Satisfaction (Continual Improvement)' - page [255](#)

Note - apart from the first two paragraphs of ISO 22313 - clause 10.2, the remaining paragraphs are basically repeats of the information already included in clause 10.1 - dealing with non-conformance and corrective action





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 may currently operate will generally no longer permit them to turn a blind eye (without some degree or other of risk to the organisation) to the consequences of not having adequately planned and resourced for how to respond to the appropriate disruption threats potentially facing them

The general expectation of the 'modern world' is that plans and resources to combat disruption must be in place - and if they are not (or are deemed inadequate), then the risks to an organisation emerging from a major disruption event without damage to its reputation and 'financial bottom line' are significant - possibly to the extent of putting the organisation out of business - in extremis

Furthermore - governments, regulators, customers & similar stakeholders / other interested parties are increasingly '*holding an organisation's top management and specialists to personal account*' for any negligent pre-preparation and / or actual handling of / response to a crisis - including one involving BC. 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 are well advised to adopt modern management 'tools' to assist in the desired response - one of which is the implementation of a Business Continuity Management System

Airlines, airports, GHAs etc. are no exception to any of the above





Deliberately Blank





APPENDIX A

CASE STUDIES

1 / SECOND GULF (IRAQ) WAR - 2003	page 267
2 / British Airways CATERING STRIKE (Industrial Action) - August 2005	page 274
3 / London Heathrow Airport - TERMINAL 5 CRISIS - March 2008	page 277
4 / British Airways CABIN CREW STRIKE - late 2009 to early 2010	page 281
5 / VOLCANIC ASH & AIRSPACE CLOSURES - April & May 2010	page 285
6 / British Airways - IT FAILURE - May 2017	page 295





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.

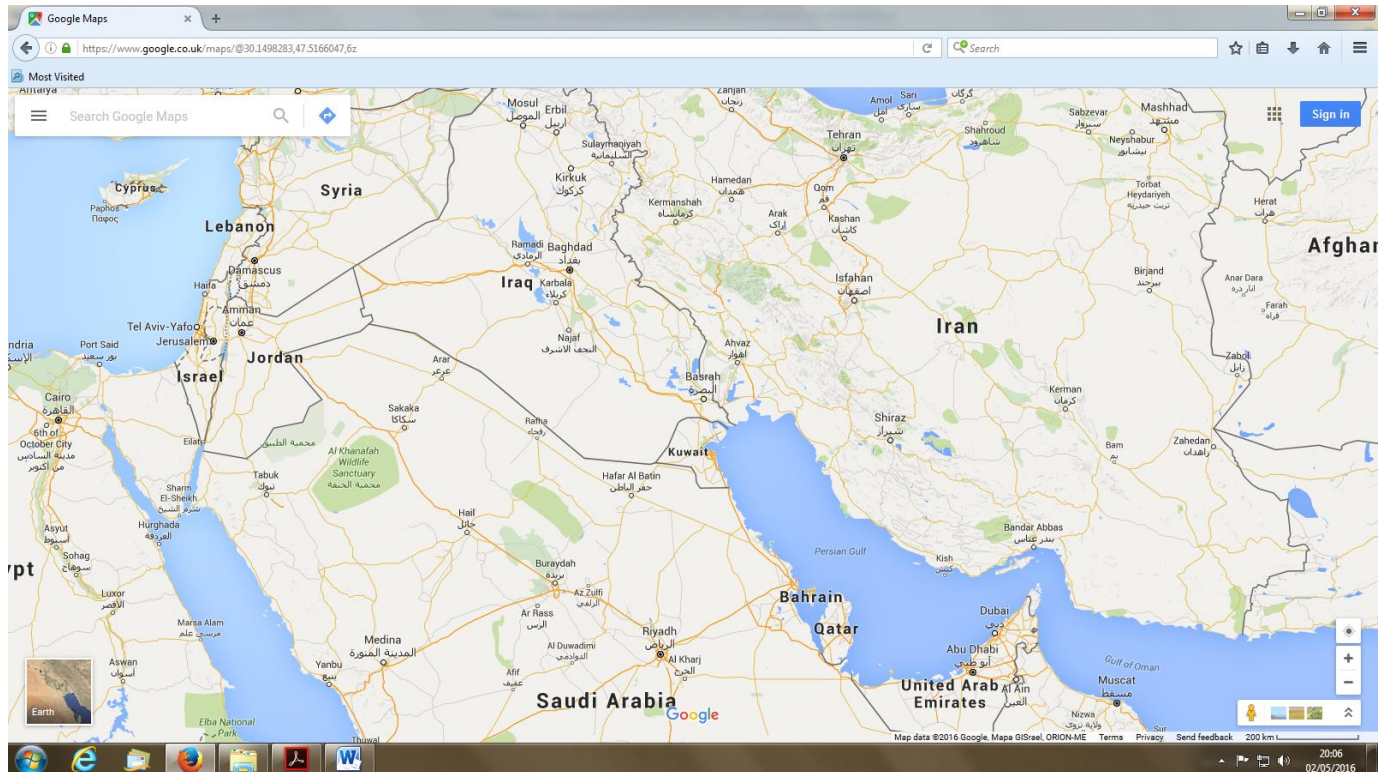
ABCX Airways is currently (January 2003) preparing for a potential major *disruption* should military action commence in nearby Iraq in the near future - such military action having the potential for serious to severe (*adverse*) operational and commercial disruption impact on airline operations

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

Prepared by ABCX Airways Crisis Response Planning Department - 20 Jan 2003





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

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 pre-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

<http://news.bbc.co.uk/1/hi/england/london/4144386.stm>

<http://www.telegraph.co.uk/finance/migrationtemp/2810670/BA-puts-catering-out-to-tender.html>





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 **pre**-planning for all forms of adequate stakeholder / other interested party communications at time of crisis. This pre-planning should include 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

<http://www.computerweekly.com/Articles/2008/05/14/230680/british-airways-reveals-what-went-wrong-with-terminal.htm>

<http://www.telegraph.co.uk/news/uknews/1583288/Heathrow-Terminal-5-British-Airways-to-cancel-flights-all-week.html>

<http://www.telegraph.co.uk/news/uknews/1583725/Terminal-5-chaos-costs-British-Airways-16m.html>





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

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

<http://www.guardian.co.uk/business/2010/jun/07/british-airways-20th-day-strike>

<http://www.bbc.co.uk/news/business-13373638>





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

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:

<http://pubs.usgs.gov/fs/fs030-97/>

http://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

<http://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

<http://www.telegraph.co.uk/travel/travelnews/7612109/Iceland-volcano-UK-airports-reopen-as-BA-claims-shutdown-unnecessary.html>

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

<http://www.telegraph.co.uk/travel/travelnews/7623988/Iceland-volcano-Inside-Thomsons-crisis-centre.html>





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

And finally - a 'tongue in cheek' solution to volcanic ash problems on aviation!



© Unknown





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://www.biznews.com/uk-news/2017/05/30/ba-crisis-management-tests/>

Article (at end of above link) written: 30 May 2017

By: Denis Fischbacher-Smith (Denis.Fischbacher-Smith@glasgow.ac.uk)





Deliberately Blank





APPENDIX B

Risk Categories - more information

There is typically no consensus on how an organisation might generically *categorise* the types of risk which could impact upon it. One method 'links together' risk in the following categories

- **Hazard Risk** arises e.g. from property / facilities, (legal) liability, personal loss exposures etc. - and is generally mitigated (treated to reduce impacts) by taking out appropriate insurance
- **Operational Risk** typically relates to 'failure' in a people associated context and also in business associated processes, systems (including ICT), controls etc. One method used to control / treat such risk is by use of Business Continuity measures
- **Financial Risk** - arising from the effects of market forces on financial assets and / or liabilities. This risk is typically sub-divided further into:
 - Market Risk
 - Credit Risk
 - Liquidity Risk.....and
 - Price Risk
- **Strategic Risk** - can come about due changing trends in the economy and society, including changes in the political and competitive environments, demographic shifts etc.

Hazard and Operational Risks might be classified as '**pure**' risk - whereas Financial and Strategic Risk might be regarded as '**speculative**' related risk

Organisations will usually categorise risk according to what it is that the organisation 'does' - so the information provided above must be regarded as typical only e.g. some will regard legal risk as slotting into the 'operational' risk category instead of the 'hazard' risk category

Moreover, such information must not be regarded as being exhaustive i.e. there will typically be more risks over and above those listed. See definition of 'Risk Category' - page [43](#)

For visual impact purposes, such categories might be envisaged as lying in 'quadrants' of a circle - as per the diagram on page [299](#). This then lends itself to better interpretation as related to 'real life'

For example, take a new (start-up) business organisation (**Company X**) which manufactures mechanical parts in **Country A**, using a largely automated production line. It sources its raw materials from **Countries B** and **C** and sells the finished product in **Country D**





- In the **Hazard Risk** quadrant, Company **X** should include 'property' related risks for its facilities, plant, equipment etc. - such risks possibly being associated e.g. with fire, natural disaster, utilities (power / electricity) failure - and so on. It should also include risks associated with injury to employees; risk of liability associated with use / quality / safety of its product etc.
- **Operational Risk** could arise from e.g. employee turnover, the inability to find skilled staff etc. There would also be 'business process' risk related (for example) to how the business manages its supply chain; ICT risks related to the automated manufacturing process etc.

Another way of expressing 'operational risk' might be:

'.....The risk of loss resulting from inadequate or failed internal processes, people and systems - or from external events - but might be more simply viewed as the risks arising (in general) from just carrying out an organisation's normal business functions.

Operational risk exists in every organisation, regardless of size and / or complexity.....'

- **Financial Risk** might arise for a number of reasons - e.g. price (currency) exchange rate risk for country **A** with regard to countries **B**, **C** and **D**; price risk for procuring raw materials and other essential supplies etc. If the country **D** customer is slow to pay its bills, liquidity (cash-flow) risk could materialise for Company **X**
- **Strategic Risk** includes competition; economic factors affecting consumer demand; political and security etc. risks in countries **A**, **B**, **C** and **D** - and so on



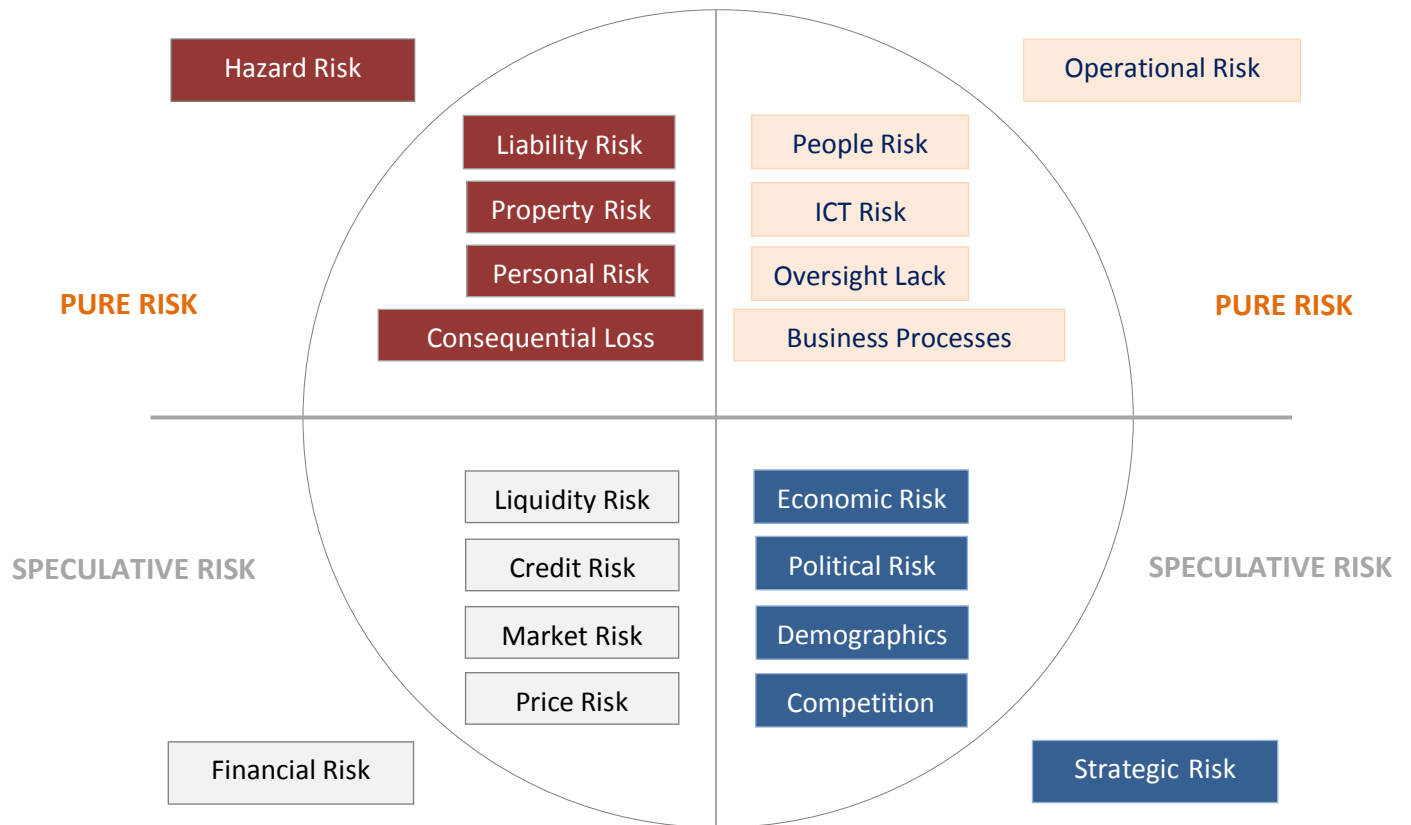


Diagram: Typical Risk Categories (List is not exhaustive)



Enterprise Risk Management

The term 'enterprise risk management' (ERM) generically describes the process of *coordinated* risk management, which places a greater emphasis on *cooperation to direct and control / manage* the *full* range of risks across an *entire* organisation. ERM thus offers a '*holistic*' framework for effectively managing uncertainty, responding to risk and harnessing opportunities (risk appetite) as they arise

Unlike previous risk management practices (which often tended to be run as separate, un-coordinated 'silos' [within an organisation]), the concept of ERM embodies the notion that risk management cuts across an entire organisation

The goal of ERM is to better understand the organisation's resistance to *all* of its key risks and thus also better manage risk exposure to the level desired (including 'risk appetite' factors) by top management

Note - in practice the dividing line between 'risk management' and 'enterprise risk management' is often blurred





© AERPS / MASTERAVCON (A H Williams) 2007 to 2018 - some rights reserved

Deliberately Blank





Appendix C

Horizon Scanning



DEFINITION

(As related to the Risk Management / Business Continuity / Contingency Planning Context)

The systematic examination of potential threats, opportunities and likely future developments
- including (but not restricted to) those at the margins of current thinking and planning

Horizon Scanning may explore novel / unexpected issues as well as persistent problems and threats



Background

An 'annual' horizon scan of appropriate, actual and potential business / organisational risks and threats is compiled (on a worldwide basis) by the UK's * 'Business Continuity Institute' (BCI) in conjunction with the UK's 'British Standards Institute' (BSI). 2017 was the 6th such scan in successive years

* Although the BCI and BSI are UK organisations, they have thousands of members all over the world - and input from same is used to compile the annual horizon scans - as is evidenced from the following extracts from the 2016 and 2017 Horizon Scans respectively:

'.....In association with BSI, the BCI Horizon Scan Report is an annual exercise which seeks to identify near-term threats to organizations worldwide. It also measures the sentiment of business continuity (BC) and resilience professionals by indicating their level of concern to different risks and threats. As a respected industry resource, the report complements in-house analysis and benchmarks horizon scanning activity among organisations across regions and industry sectors. Data cited in this report was obtained from a survey which began in October 2015 and ran for eight weeks. 568 organizations from 74 countries participated in this study.....'

'.....In association with BSI, the BCI Horizon Scan Report is based on an annual study which tracks near-term threats to organizations across industry sectors globally. In its sixth edition, this study measures concern over specific threats as reported by business continuity and resilience professionals. The report also captures disruption caused by these threats, offering a basis of comparison between the level of concern and actual incidents. Over the years, this report has become a highly anticipated industry resource as it complements in-house analysis and assists horizon scanning activity. The report features results of a survey which was distributed from October 2016 and ran for four weeks; 726 organizations from 79 countries participated in this study.....'

The general objective of the horizon scan is to confirm older / current types of risk (i.e. are they still relevant / accountable?) and to also try to identify and quantify new types of risk materialising, which might eventually test societies, organisations etc. worldwide, to a greater or lesser degree

By its very nature the 'forward-looking' aspect of horizon scanning is typically imprecise (in a similar way to the imprecision of longer range weather forecasting). However, it is significantly better than nothing and, as it is updated annually, can be used by risk management, business continuity and emergency / incident planners to tentatively update their risk registers and contingency plans - where thought appropriate

It is strongly recommended that all involved closely with risk management, business continuity and emergency / incident response planning acquire and take due note of said horizon scans.

They would also be well advised to conduct and act on their own 'bespoke' horizon scans - where the circumstances of their own societies, organisations etc. so require

To find the BCI / BSI horizon scans on the internet, simply conduct a search using the following words. (The 'year' to insert should be the one that you are interested in of course):

'.....BCI / BSI horizon scan 2018.....'

