EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels 28/05/2010
HR.DS (ARES) 288993

European Commission

Information System Security Policy

C(2006) 3602

GUIDELINES ON BUSINESS CONTINUITY MANAGEMENT

Version 1 of 28/05/2010

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1

TABLE OF CONTENTS

1. INTRODUCTION

In line with the Secretary General 'Framework for Business Continuity Management (BCM) in the Commission' this document describes guidelines for implementing the

Business continuity management system at the Commission with an emphasis on Information System Security. It is not a replacement of the SG framework but a complement to it written in the context of the security policies.

References to the SG framework are done and numerous repetitions appear to make this document as standalone as possible such that the reader is not obliged to go back and forth between the 2 documents to understand the process.

The Business Continuity Management is an overall process determining possible impacts threatening the Commission and leading to the subsequent adoption of a continuity framework for instilling resilience into its functions, processes and activities. It also gives a capability to withstand interruptions of its business operations and recover from them so that the interests of its stakeholders are preserved.

The improvement of resilience is achieved by the assessment **in advance** of the possible impacts of various types of interruption to the business functions, processes and activities, and, hence, by giving priorities to the effort to resume them, based on their value to the Commission. These efforts can be in various areas like staffing, facilities, information systems, network and security.

Without overlooking the other scales of resilience, the BCM is dedicated to the development of a Commission-wide resilience to survive the loss of a part or all of its business functions, and also of other resources like staff and equipment. This Commission-wide development of resilience has to consider the overall organization of the Commission in DGs and the geographical spread in many buildings and has to be done throughout the hierarchy from the top management to the bottom.

It is also important that the BCM is understood as a process completely integrated into the Commission management and organization.

2. GUIDELINES OBJECTIVES

The purpose of this document is to enable the Commission to withstand interruptions to business functions, and to protect mission-critical business functions from the effect of major failures of information systems or disasters and to ensure their timely resumption.

3. BACKGROUND INFORMATION

3.1. Context

See introduction.

3.2. Risk assessment

As indicated in the SG's framework, events such as 9/11, the threat of a global flu pandemic or less dramatic but equally damaging threat to staff, building or information systems all highlight the need for organizations to prepare for major potential disruptions to their activities. Business continuity management is the process that helps manage the risks to the effective operations of the organization.

3.3. Definitions

Organization: in this document 'organization' will be used as the generic name to refer to the entity for which the BCM has to be established. It can be used instead of a DG or a family of DGs.

Activity or function: process or set of processes that are implemented in an organization to produce or support one or more services in line with the organizational objectives. These activities, functions or processes depend on the existence or availability of their supporting components like facilities, buildings, IT infrastructure (including voice and data communications), hardware and software, networks, vital records, data, business partners and staff. In line with the Secretary General's 'Framework for Business Continuity Management in the Commission' the term 'function' will be used as a generic term for the activities, services and infrastructures.

Process (or function) mapping: a thorough understanding of the enterprise business process (or function) allows the planner to see how mega-processes (-functions), major processes (-functions), and major sub-processes (-functions) operate and how they correlate one to another, map across the organization, and interrelate in terms of their availability requirements.

Business continuity management (BCM): holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its stakeholders, reputation or value creating activities.

Business continuity planning (BCP): a process that identifies all critical functions, services and activities that must be accomplished to enable an organization or functional business area to continue business and business support functions during a time of disaster or serious disruption (e.g. power outages, natural disasters, accidents, acts of sabotage, or other incidents).

Business Impact Analysis (BIA): process of analysing business functions and the effect that a business disruption might have upon them.

Disaster recovery planning (DRP): a process that identifies all activities that must be accomplished to respond to a disaster or serious disruption and to recover the IT infrastructure of an organization to its normal operational level.

Maximum Tolerable Period of Disruption (MTPD): this is the duration after which an organization's viability will be irrevocably threatened if a particular process, product or service delivery cannot be resumed.

Recovery Time Objective (RTO): this is the target time set for resumption of product, service, performance of an activity or a function, or an information system after an incident. The RTO has to be less than the corresponding MTPD.

Recovery Point Objective (RPO): is the point to which information must be restored to enable a function to operate once it is resumed. It refers to how current or fresh the data is after a disaster.

Disaster radius: refers to how extensive the disaster is in terms of geographical spread.

Time-critical business functions: business activities or information that could not be interrupted or unavailable for a specified time (MTPD) without significantly jeopardizing the operation or the reputation of the organization

High-availability: a resilience level of a system resulting from its design in such a way that it is supposed to meet at least its business requirements.

Remark on DRP and BCP: while DRP identifies the IT assets and concentrates on the recovery of the IT infrastructure, the BCP concentrates on maintaining or performing business when the IT assets are unavailable. The business resumption process and the IT

recovery identified in the DRP need to be synchronized. The BCP will identify equipment, processes, personnel and services required to keep essential business functions operating, and it will describe the process required to transition business back on to the recovered IT infrastructure.

4. SCOPE

As indicated in the 'Framework for Business continuity management in the Commission' published by SG {SEC (2006)898}, the scope is the preparation for major disruptions affecting the Commission itself, i.e. its activities, staff, buildings, information and other assets. It does not address major incidents outside the Commission, except to the extent that these also impact on the Commission's ability to operate normally.

The overall scope for Business continuity management covers the Disaster Recovery Plans which are dedicated to the recovery of ICT systems and activities in case of their major disruptions.

5. ROLES AND RESPONSIBILITIES

The overall responsibilities for Business Continuity Management in Commission services are described in Section 2.3.2 and mainly section 3 of 'Framework for Business continuity management in the Commission' published by SG {SEC (2006)898}.

The system owner has the ultimate responsibility (accountability) for all security aspects for the information system (s)he owns as described in the Implementing Rules.

Hence, within the context of overall Business Continuity Management encompassing his system, the system owner is accountable for the business continuity management aspects of her/his information systems but he can delegate responsibility of their specification, implementation, operation, training, testing and monitoring to other roles.

In case of subcontracting any aspect of his/her system, the system owner must ensure that the adequate business continuity requirements are mandated in the formal agreements.

6. POLICY STATEMENTS

Policy objective 9.1.1.: A managed process shall be developed and maintained for business continuity that addresses the information systems security requirements needed for the business continuity for the Commission.

Policy objective 9.1.2.: Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences for information systems security.

Policy objective 9.1.3.: Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes and other important business processes.

Policy objective 9.1.4.: All plans must be drafted under the business continuity framework defined by the Secretariat-General.

Policy objective 9.1.5.: The IT aspects of business continuity plans must be tested and updated regularly to ensure that they are up to date and effective.

7. STRUCTURE OF THE DOCUMENT

This document is structured along a multiple step approach that is quite common in the BCM practices:

- Scope of business continuity management.
- Business Impact Analysis.
- Risk assessment or evaluating threats to most critical functions.
- Strategy of business continuity.
- Developing and implementing a BCM response.
- BCM training and awareness.
- Types and methods of exercising BCM plans.
- Exercising, maintenance and audit.
- Assurance, compliance, metrics (to be provided)

In the rest of the document 'organization' will be used as the generic name to refer to the entity for which the BCM has to be done. It can be used instead of a DG or a family of DG's (like the HR.DS family of DGs with similar characteristics).

In line with the Secretary General 'Framework for Business Continuity Management in the Commission' we will use the term function as a generic term for the activities, services and infrastructures.

8. SCOPE OF BUSINESS CONTINUITY MANAGEMENT

The scope of BCM contains all the most critical functions of the organization. The scope is defined through the following steps.

8.1. Obtain key business objectives

The very first step is to establish a clear statement of the key business objectives of the Commission and/or of the organization and to understand how they are achieved.

8.2. Identify mission-critical functions to include in BCM scope

It is then necessary to identify the functions of the organization that really need to be included in the scope of the business continuity management. Setting the scope is to avoid wasting time with analysing functions that are not mission-critical and keep focusing on the functions that are essential to the accomplishment of the objectives.

A list and description of the functions that are mission-critical need to be established in line with these business objectives. These functions have to be identified at an appropriate level of details. Some guidelines for understanding the organization from high-level functions (processes, services, infrastructures or activities) down to lower-level sub-functions tasks is given in appendix 1.

Without going into many details, the following questions can be considered to quickly identify the core functions that should be included in the scope of BCM:

(a) Does this function support a business objective of your organization? (Weight Wa=)

(b) Is this function performed only by your organization, or is it also performed by other organizations within the Commission? (Weight Wb=)

(c) Does another organization, vendor, partner, government or external organization depend on this function or successful completion of its function? (Weight Wd=)

(d) Is there a potential either for loss of reputation or adverse publicity or for political problems in case of this function not running? (Weight We=)

(e) Is there a potential for loss of life or injury to personnel, business associates, or externals if this function is not carried out? (Weight Wf=)

(f) Is there a potential for significant financial loss to the organization if this function is not carried out? (Weight Wg=)

(g) Is there a potential for significant fines, litigation, jail terms, or other punishment for non-compliance to a required regulatory or contractual requirement? (Weight Wh=)

(h) Is non-compliance tied to a specific threshold for downtime of this function? (Weight Wi=)

(i) Is non-compliance tied to a specific for data loss or disclosure of sensitive information for this function? (Weight Wj=)

(j) Is this function carried out by key (critical) personnel within the organization? (Weight Wk=)

(k) Are other personnel within the organization available and capable of performing the function in the absence of key personnel? (Weight Wl=)

(l) What priority would your organization give this function within the entire Commission? (Weight Wm=)

(m) Is it a perceived high-risk location (due to the proximity to potentially dangerous industrial area or prone to physical threat like flooding) (Weight Wn=)

By giving a weight to the questions above and scoring by 0 or 1 depending on the answer (either yes or no or based on a threshold value), you can provide a weighted sum which can give a 'criticality level'. Above some value X the function is eligible to be included in the scope. Below the value X, the function should not be included in the Business continuity management programme.

The appendix 2 provides a tool to assess the criticality of a function with an example of weights and scores. It is possible to customize it based on the organization's reality by using customized weights.

After the decision has been made about which services and related functions are within the scope of the BCM programme, the BIA can be undertaken to understand the impact of the failure to deliver the function, as explained in the next section.

9. BUSINESS IMPACT ANALYSIS

9.1. Overview

Once the scope is determined the Business Impact Analysis is the essential step on which the whole Business continuity management is built.

It allows the identification and the assessment of the business impact of a loss, interruption or disruption of the business functions that are within the scope of BCM. Its output allows defining an appropriate continuity strategy based on a prioritization of functions to recover.

The outcome and deliverables of the BIA for each function within the BCM scope:

- Document the impacts over time that would result from loss or disruption of the function.
- Determine the Maximum Tolerable Period of Disruption (MTPD) and its justification. The MTPD is the duration of function disruption after which an organization's viability is threatened if the function cannot be resumed.
- Identify the dependencies (both internally and externally) that are required to enable the function to operate effectively. In fact functions may depend for their delivery on the 'support' of other internal and external functions or processes, which must also be analysed.

So, after mapping the functions on their support resources (i.e. IT applications, networks, facilities, third parties, staff) or other supporting functions, the MTPD can be translated into requirements for support resources needs and availability or for other supporting functions.

9.2. BIA methods

There are 2 possibilities to assess the MTPD for a function and to determine its category:

- Either using the questionnaire and tips given in the two documents provided by SG (see 'Framework for Business continuity management in the Commission – SEC(2006)898' and 'Guidance on how to prepare a business continuity plan Version 2 – 10 July 2006').
- Or using a formal method derived from the formal method on asset classification. This method is described in appendix 3.

9.3. Categories of functions based on their MTPD

For the purpose of Business continuity within the Commission functions are categorised based on the MTPD, as follows:

- **Critical functions** - these are activities, services and infrastructures that cannot be interrupted at all, or which need to be restored within 1-2 days; without these, The Commission's operation would be significantly jeopardised.

- **Essential functions** – these are activities, services and infrastructure where a short interruption can be tolerated (up to 1 week), but after which the Commission's operations would be disabled.

- **Necessary functions** – these are activities, services and infrastructure that the Commission could afford to interrupt for at least a week without serious effects, but that should be restored as soon as circumstances permit.

These definitions are intended to facilitate the identification of priorities when it is impossible to maintain all normal activities and do not involve value judgements about the importance of these and other functions under normal working conditions.

9.4. Supporting resources recovery requirements

The resources, infrastructures and other sub-function supporting each function must be identified in parallel with the BIA. This consists in the collection of information on the numbers of resources required to resume and continue the function at a service level required to satisfy the organization obligations and within the MTPD.

This information feeds directly into the Business Continuity Strategy stage. The resource requirements will provide the data to evaluate alternative recovery solutions for adequacy of size and performance.

The resources to consider are:

- People or staff resources (numbers, skills, knowledge).

- Premises with identification and description of sites and facilities.

- Technology – IT resources: applications, networks, equipment.

- Electronic or paper-based information that must be available, including previous work or work in progress and level of currency of this information.

- External organization services, business partners, contractors.

- Supplies.

- Civil emergencies.

10. RISK ASSESSMENT OR EVALUATING THREATS TO MOST CRITICAL FUNCTIONS

10.1. Purpose

After the Business Impact Analysis phase, a risk assessment has to be performed to determine the potential threats an organization might experience and the potential

for each threat to occur. The risk assessment has to be done in **each location** where the organization houses its mission-critical functions identified by the BIA.

While the BIA provides the business value of a function in a worst case situation, the risk assessment allows considering the impacts of realistic threats to the function and choosing adequate measures, either to reduce the impact and duration of the disruption, or to increase the function resilience to specific threats.

In a BCM context, the level of risk has to be assessed specifically with respect to the most important functions and the risk of a disruption of these. There is a need to first focus on the Critical and Essential ones identified in the BIA, and on the Necessary functions in a second stage. These functions are supported by resources such as people, premises, technology, information, supplies and stakeholders. The organization has to consider the likelihood of threats to these resources, the vulnerabilities of each resource, and the impact that would arise if a threat became an incident and caused a business disruption.

It is often difficult to scope a risk assessment across an entire organization. By focusing on the resources required to operate the organization's most important functions (i.e. critical and essential following a BIA), the focus on the Risk assessment can be reduced to a more manageable scope.

After assessing the threats, vulnerabilities and impacts it is possible to decide a risk strategy. In this context deciding a risk strategy consists in accepting, reducing, transferring or avoiding the risk, i.e. by implementing measures to reduce the likelihood or mitigate the impact of these threats.

Business continuity strategy is a very important measure that can be decided to reduce the impact of a disruption. The other measures resulting from the risk assessment would be additional to a business continuity strategy and certainly have a very positive effect on business continuity. Similarly a business continuity strategy does not replace the other measures but can be considered as an important measure amongst the others.

So to summarize the purpose of risk assessment is threefold:

- Identify the internal and external threats that could cause a disruption and assess their likelihood and impact.
- Prioritise the threats according to an agreed formula.
- Set up a risk management control programme and action plan.

The following sections are based on the "Standard on risk management" document and explain the main steps for a risk assessment in the context of BCM.

10.2. Step 1: Identification of threats

Need to identify the threats, internal or external, that could cause the disruption or loss of the organization's mission-critical functions and their supporting resources.

Examples of threat with the potential to escalate into a disaster and crisis are given below to help build the list. Not all of these threats are likely or relevant in the locations of the Commission buildings. However the predictability aspect and the likelihood of the individual threats are considered in the next section. This list does not pretend to be exhaustive.

Acts of nature or natural threats:

– Earthquake: is your function carried out in a location prone to earthquakes?

– Flood or rising water: do you think that a flood or rising water can threaten your functions or supporting resources?

– Extreme weather conditions (e.g. hail, freezing rain, strong wind and drought): can extreme weather conditions have an impact on the functions or resources?

Accidental threats and environmental threats:

– Fire: do plans exist to counter fire?

– Power outage: what level or duration of power outage could threaten the functions and supporting resources?

– Airplane: is an airplane crash a possible threat?

– Explosion (whatever cause): what could be the impact of an explosion inside the premises or outside the premises?

– Water or liquid leaking: can water or liquid leaking threaten the functions and supporting resources?

– Nuclear accident: is there such a risk around the location.

– Chemical pollution from risky vicinity: is there a high-risk industry (chemical, petroleum) close to the location of the functions?

– Climate failure: does you plan consider problems due to climate failure like overheating?

Deliberate threats:

– Arson: does your plan consider arson as a threat to functions and supporting resources?

– Bombing: are your locations a target for this type of attack?

– Sabotage: same question as for bombing, either from insiders or outsiders?

– Terrorism: same question as for bombing, either as a specific target or a blind attack?

– Vandalism: same question as for bombing, either from insiders or outsiders?

– Civil disturbance/riot: can civil disturbance or riots have an impact on the availability of your functions or supporting resources like staff or suppliers?

– Strikes: can external or internal strikes have an impact on the availability of your functions or supporting resources, like staff or suppliers?

– Workplace violence: can this have an impact on your functions and supporting resources?

– Actions from staff: threats from disgruntled employees like strike or sabotage

Incidents potentially escalating to a serious disruption.

– Cash or financial problem: can a cash or financial problem have an impact on the continuity of your functions or the availability of supporting resources?

– Supplier/vendor: can a problem with your supplier/vendor like bankruptcy or strike have an impact on your functions?

– Bad disaster recovery exercise: are your sure that a disaster recovery exercise does not disrupt your functions?

– Major disease outbreak like flu pandemic.

– Unexpected death or long absence of key people: Are there key people whose long absence or death can disrupt your functions?

– No access to the premises: how long can the access to the premises be impossible without jeopardizing the functions?

– Massive virus attack

10.3. Step 2: Identification of the vulnerabilities to identified threats

We must answer the following question for each function and its supporting resources: how vulnerable is each function to the threats identified as predictable for the location?

In other words what are the vulnerabilities of the supporting resources of a function that can be exploited by the threat to disrupt the function or to make a disaster?

In fact, vulnerabilities might occur as weaknesses within the resources and can then be exploited by the threats: e.g. single points of failure, inadequacies in fire protection, insufficient electrical resilience, inadequate staffing levels, holes in IT security and limited IT resilience.

It is essential to figure out the possible scenario(s) of a threat exploiting one or multiple vulnerabilities of the supporting resources to seriously harm the function. A threat without a corresponding vulnerability is ineffective and vulnerability without a corresponding threat is not really a weakness.

10.4. Step 3: Assessment of the likelihood of each threat and related vulnerabilities (probability or frequency)

The likelihood that the related threats and vulnerabilities come together to disrupt the function needs to be assessed.

Scoring system for likelihood of threats and vulnerabilities

The likelihood of each threat and related vulnerabilities will be assessed using the scoring system described in the following table. This table contains a numerical scale and a qualitative scale with the six definitions.

Numerical scale	Qualitative scale	Definition
5	Almost	Certain the event is expected to occur in most circumstances (more than one in 12 months)
4	Likely	The event will probably occur in most circumstances (once in 2 to 5 years)
3	Moderate	The event should occur at some time (once in 5 to 7 years)
2	Unlikely	The event could occur at some time (once in 7 to 10 years)
1	Rare	The event may occur only in exceptional circumstances (less than once in 10 years or more)
0	Irrelevant	Not applicable

In this context, 'event' means the association of a threat exploiting one or more vulnerabilities to materialize into a disruptive incident or a disaster. This likelihood assessment has to take account of the existing measures, which have already been implemented to reduce threats and vulnerabilities.

Guidance for likelihood assessment

The following guidance lists parameters and sources of information that can be considered for likelihood assessment vary depending on the kind of threat. The text is based on the Standard on Risk Management document.

- Deliberate threats: the likelihood of deliberate threats depends on the motivation, knowledge, capacity and resources available to possible attackers and the attractiveness to some resources supporting the functions.

- Accidental threats and environmental threats:

  – The likelihood of these threats can be estimated using statistics of past occurrences and experience, for example provided by insurance company or published disaster frequency statistics.

  - This likelihood can also be related to the organization's proximity to sources of danger such as major roads or rail routes, factories involved in dangerous materials such as chemical or petroleum.

  - Last but not least human errors (one of the most common accidental threats) and equipment malfunction can influence the likelihood.

- Natural threats: insurance company statistics or other published statistics on earlier events that show when such acts of nature have occurred for a defined period (e.g. a 100-year period for earthquake). They do not say when it might occur but provides a likelihood it happens in a defined period.

- Other source of statistics:

  - The best source of crisis statistics would be from various industry organizations that keep track of the instances where "crises" have affected an organization in that industry. However these statistics are not always available to organizations and people outside the industry. Also there are some statistics on crisis available from government agencies.

  - Past incidents of the organization: nature and frequency of past incidents experienced in the organization can help in the likelihood assessment. This requires having an incident management process in the organization.

  - New development and trends: reports and news available on the Internet, newsgroups or specialised organizations can be a source of trends on incidents statistics

10.5. Step 4: Estimate the impact of the threat using a numerical scoring system

Scoring system for impact assessment

The impact of each threat exploiting one or more vulnerabilities will be assessed using the scoring system described in the following table. This table contains a numerical scale and a qualitative scale with the five definitions.

In the risk model suggested here the risks assessed are examined with the existing measures in place. So the impact of a threat occurring has to be estimated considering the existing measures, which have already been implemented to reduce the impact.

Numerical scale	Qualitative scale	Definition
5	Very High	From exceptionally grave to catastrophic damage: complete disaster with potential to collapse function
4	High	Serious damage: event that can cause long term disruptions of important part(s) of the function
3	Medium	Significant damage: event that with substantial management can

		be endured
2	Low	Moderate damage: event that with appropriate process , can be managed
1	Very low	Negligible or no damage: any consequence can be readily absorbed

10.6. Step 5: Calculation of the risk

The risk is calculated by combining the scores for impact and likelihood of each threat according to the following formula:

Risk = threat likelihood * {(impact score)**1.45}

This method relates the impact score and the likelihood of disruptive incident or disaster occurrence (threats and vulnerabilities coming together to cause a particular event, taking into account any existing measures).

The table below gives the result of the calculation. The exponent of the impact score is proposed to be 1.45 and allows providing more weight to the impact score: it is possible to change this exponent to fit the organization reality.

This table allows ranking the different threats based on their overall risk score.

It is possible to classify the risks into 4 categories as explained below the table:

- 'High' if the risk score is above 21.
- 'Significant' if the risk score is more than 11, but less than or equal to 21.
- 'Moderate' if the risk score is less than or equal to 11, but more than 5.
- 'Low' if the risk score is less than or equal to 5.

Note: the determination of these categories can be adapted to the reality of the organization by adapting the limits of the categories.

Risk assessment matrix							
Impact		Likelihood of threat occurring					
		5	4	3	2	1	0
		Almost	Likely	Moderate	Unlikely	Rare	Irrelevant
5	Very high	52	41	31	21	10	0
		High	High	High	Significant	Moderate	N/A
4	High	37	30	22	15	7	0
		High	High	High	Significant	Moderate	N/A
3	Medium	25	20	15	10	5	0
		High	Significant	Significant	Moderate	Low	N/A
2	Low	14	11	8	5	3	0
		Significant	Moderate	Moderate	Low	Low	N/A
1	Very low	5	4	3	2	1	0
		Low	Low	Low	Low	Low	N/A

High	more than 21
Significant	<=21 but >11
Moderate	<=11 but >5
Low	<=5
N/A	

10.7. Step 6: Risk strategy or treatment

The results of the risk assessment allow the organization to identify countermeasures of loss mitigation and risk treatment, either to reduce the likelihood of a disruption, or shorten the period of disruption, or limit the impact of a disruption of the organization's activities.

Not all risks can be prevented or reduced to an acceptable level for the organization compared to its 'risk appetite'[1]. So the organization has to choose **one or more or all** of the following risk strategies for each function that has been risk-assessed. The decision of a risk strategy has to be based on a cost/benefit balance and to be approved by the Director General of the organization.

Preliminary and important remark: even if Business Continuity is decided as a risk strategy, the other possible strategies must not be overlooked.

Accept the risk

This strategy consists in tolerating the existing level of risk without any further action being taken, i.e. without adding any measures to the existing ones to reduce the threat, the impact or the likelihood of any vulnerabilities being exploited by a threat.

[1] The organisation 'risk appetite' or 'risk tolerance' is the amount of risk an organisation is prepared to accept and drives the level of action it will take to control identified threats.

The management will typically decide on this strategy in the following situations:

– No measure can be identified to reduce the risk or very limited ability exists for that type of risk. In this case the response may be to tolerate the existing risk level if the management considers it to be acceptable.

– The cost of implementing the measure outweighs the potential loss or cost due to the threat materialising through vulnerabilities. In this case also the response may be to tolerate the existing risk level if the management considers it to be acceptable.

If we refer to the risk assessment matrix, it is recommended:

– The acceptance of risk may be allowed in the two situations above typically if the risk level is 'low' or 'moderate'.

– The acceptance of risk should not be allowed for risk levels of 'high' or 'significant'.

– However the decision to accept is the responsibility of the management and they can decide not to follow these two rules.

Reduce the risk (including business continuity)

This strategy consists in introducing more measures in addition to the existing ones so that the risk level is reduced to an acceptable level or as close to it as possible.

These measures can be any measure that improves the resilience of the activity to disruptive events or reduce the impact. One of these strategic measures is Business continuity, which is developed longer below.

The other measures can be dedicated to any of the resources supporting the activity and, consequently, they can fall into the same categories as the resources: organizational, people related, environmental, hardware or software controls, physical or building related, process.

For example in case there is a risk due to a key activity that can only be carried out by an individual, the additional measure would be to train one or two other individuals to make sure the activity is not disrupted in case of absence or disappearance of the key individual.

Measures can reduce the assessed risks in many different ways, for example by

– Reducing the threats: e.g. by changing a risky process.

– Reducing the likelihood of the vulnerability being exploited by the threat: for example by replacing normal windows by armoured ones.

– Reducing the possible impact of the threat occurring (e.g. sprinkler systems to limit destructions).

– Detecting unwanted events (e.g. installing an intrusion detection system), reacting to, and recovering from them, for example by deciding the adoption of a Business continuity strategy.

Business continuity

This strategy consists in defining all the business continuity plans that must be followed to put back the function into service after a major disruption.

If business continuity is a chosen strategy for a key activity, a Recovery Time Objective (RTO) should be established and the continuity strategies should be evaluated against this objective (see section 11).

However other potential measures to reduce the risk must not be overlooked if a BCP strategy is adopted as they should be taken in addition to BCP as long as these measures are justified after balancing their cost versus benefit. In fact reducing the risk by these other measures is very likely to have a positive effect on business continuity.

If we refer to the risk assessment matrix to decide on a BCP strategy, the following guidelines are given:

– BCP strategy must be considered if the risk level (remaining after additional measures are implemented) is 'high' or 'significant' (except if the corresponding impact is low).

– BCP strategy can be considered if the risk level is 'moderate', mainly if the corresponding impact is 'very high' or 'high'.

– BCP strategy is not a priority if the risk level is 'low'.

– However the decision on a risk strategy is the ultimate responsibility of the management who can have good reasons not to strictly follow these rules.

Transfer the risk

Risk transfer is a strategy when, either it is difficult to reduce or control the risk to an acceptable level, or it can be more economically transferred to a third party that is more capable of effectively managing the risk.

This option is particularly good for mitigating financial risks or risks to assets.

But it is important to note that some risks are not (fully) transferable; in particular, it is generally not possible to transfer reputation risk, even if the delivery of a service is contracted out.

There are several mechanisms for transferring continuity risk to another organization:

– The use of insurance

  The purchase of insurance may form part of a risk treatment strategy and will provide some financial compensations for loss of assets, increased costs of working and protection of associated legal liabilities.

  However insurance may not provide cover for the full expense of losses or damage (e.g. uninsured incidents, damage to brand or reputation, impact on stakeholder value and human consequences). So there is an element of residual risk as there will be conditions and exclusions which will be applied, depending on the type of occurrence for which an indemnity is not provided.

  A financial settlement alone is unlikely to fully protect the organization in a manner that satisfies stakeholder expectations.

  Insurance cover is more likely to be used in conjunction with one or more other risk strategies.

  Example of typical insurances:

    'All risks' insurance to compensate for the assessed value of the damaged or lost physical assets and electronic records.

    Business interruption insurance to compensate for the 'increased cost of working' during resumption.

    'Key man' insurance to provide a sum to compensate for the loss of key individual(s) from the business due to death, injury or resignation.

    Liability insurance to provide protection for liabilities incurred including those associated with employees and third-party property and people.

– Intra-Commission sourcing or outsourcing partners

  Intra-Commission sourcing or outsourcing partners to handle critical business assets or processes can also be a risk strategy, but in this case, contractual arrangements must be settled to ensure that the duties, responsibilities, security and performance requirements are enforced through Service Level Agreements, and their related monitoring and measurements.

  Be careful that there is some residual risk as the ultimate responsibility for the activity or part of it remains with the organization because the risk to the organization image and reputation cannot be transferred to either intra-Commission sourcing or outsourced providers.

  In addition outsourcing an activity may decrease some types of risk by increasing or unveiling others that must be assessed and managed.

– Asset restoration services

  Asset restoration services are provided by a range of specialist companies who can minimise damage after a fire and flood to papers, equipment and buildings. These firms may provide an advance registration service and advice, as well as being available on request post incident.

If we refer to the risk assessment matrix, the decision on a risk transfer strategy can be considered for the risk levels 'high', 'significant' and 'moderate' when it is possible to limit the financial impact of a threat or the risk can be managed better, fully or partly by another organization.

Avoid the risk

Risk avoidance describes any drastic action where the activities or objectives are changed or suppressed to avoid any risk occurring. Risk avoidance needs to be balanced against the business, regulatory or contractual needs of the organization.

In some circumstances it might be appropriate to change, suspend or terminate the service, product, activity, function or process. This option should only be considered if there is **no conflict** with the organization's objectives, statutory compliance and stakeholder expectation. This approach is most likely to be considered if a product, activity, function or process has a limited lifespan.

10.8. Step 7: Risk treatment plan, priorities and sign-off

Prioritize the risks for implementation plan

After defining the strategies for treating the risks related to all critical and essential activities, the organization has to define an implementation plan of these strategies.

This implementation is recommended to be done based on priorities at three levels:

– First prioritize based on the risk score starting with the high risk threats.

– Second within a same level of risk, implement first the measures related to threats on activities that would most quickly disrupt the business.

– Third concentrate on the threats which are easier to control. For that purpose it is possible to assess a parameter 'Ability' to control on a five scale 1 to 5 (1 difficult and 5 very easy to control). Then the threat with a score of 5 should be dealt with first.

Sign off

The Director General or his deputy should formally sign-off the following results after making sure that the work has been appropriate and is a true reflection of his risk vision and appetite of the organization:

– The documented list of critical and essential activities and their MTPD resulting from the business impact assessment,

– The documented risk assessment outputs, and risk treatment strategies and priorities, and more specifically the strategic decisions to reduce, transfer or avoid the risks

– The documented 'acceptance' of identified risks that are not addressed.

11. STRATEGY OF BUSINESS CONTINUITY

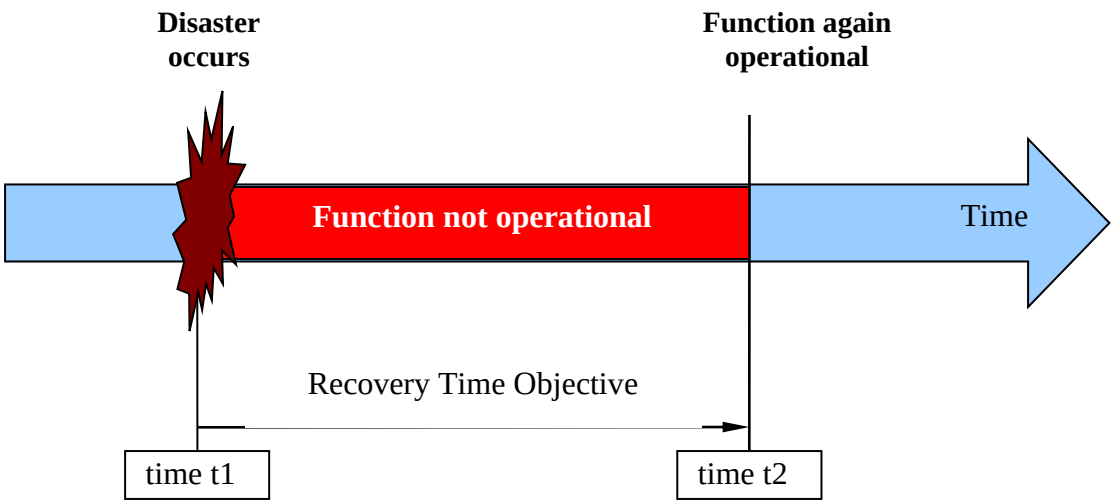
A business continuity strategy has to be defined as a complex strategy for the organization taking in account tactics and strategy of every key function for which business continuity is one of the strategies chosen after the risk assessment.

11.1. Recovery Time Objective and Disaster Radius

The starting point for a function strategy is the Maximum Tolerable Period of Disruption (MTPD) of the function determined in the BIA phase.

Considering that the MTPD is the point at which the organization will just survive when recovering a key activity, there is a need to have some margin and to define a shorter recovery time called the **Recovery Time Objective** to take account of unexpected problems during a recovery.

A Recovery Time Objective has to be defined for every key function for which business continuity is one of the strategies chosen after the risk assessment.



The continuity strategy must be done taking into account the extent of the disaster in terms of geographical spread, which is called **Disaster Radius**. In fact the recovery site and other resources necessary for the recovery must be chosen beyond that distance ensuring that they are not affected by the same disaster.

The continuity strategies for the function and all its supporting resources (or supporting functions) will be evaluated against this function **RTO**.

The choice of strategies and the final decision depend on several factors:

– Cost versus benefits and also versus cost of recovery.

– Geographical spread of the organization (DGs or family of DGs).

– Minimum separation distance between the main site and possible recovery sites.

– Risk of recovery versus benefit.

All organizations are different and all disruptions are different so 'No one size fits all' in terms of which types of resource are involved and which strategy to consider. So the following subsections provide some guidance to define the choice of tactics for the types of resource potentially supporting key functions.

It is advised to define the resources requirements for every key function in a first stage and, then, to carry out a consolidation of the resource requirements amongst all key functions to recover in case of a specific disaster.

The following sections provide the guidelines for defining continuity requirements for the potential types of resources:

– People or workforce and skills.

– Premises or worksites.

– Supporting technologies (services).

– Strategy for information/data.

– Telephony continuation and redirection.

– Equipment and supplies.

– Human welfare.

– Emergency services liaison.

– Resource consolidation amongst all key functions.

11.2. People or workforce and skills

The information identified in the BIA phase about 'supporting resources recovery requirements' allows deciding on the strategy to maintain the core skills and knowledge all the time and even in case of any disruption of the key function. This can imply the following tactics depending on the type of important disruption:

– Document the way in which the key functions must be carried out to allow other people with a minimum of skills to perform it in the absence of a key individual.

– Avoid the concentration of skills by physically separating people with the same core skills.

– Make sure that more than one individual have the required core skills by training: for example multi-skills training of staff.

– Using third-parties to provide occasional or permanent use of core skills if it is not possible to only rely on internal staff. This reliance of outside support must be submitted to contractual Service level agreements to ensure continuity of these skills availability.

– Foresee the need for succession planning of key individuals and organize it.

11.3. Premises or worksites

Worksite strategies can vary significantly from one organization to the other due to their different objectives, key functions, size and geographical base. Moreover different types of disruptive incidents and threats could require the implementation of different strategy options.

However the most determining factors in the choice of worksite strategy options are the **RTO** of the key function and the extent of the disaster in terms of geographical spread, i.e. **Disaster Radius**. In fact the recovery site must be chosen beyond that distance ensuring that both sites are not affected by the same disaster.

Then cost and availability will be the other determining factors guiding the strategy choice as described below.

11.3.1. RTO of several months

This RTO allows leaving the decision until after the incident. This gives time for buildings to be found and utilities to be installed after the incident with just a minimum of planning and preparation. This site has to be found at a distance so that it is not impacted by the same incident. For example it could be one of more of the following:

– A site owned by the organization or another organization within the Commission.

– A commercial recovery site to be found.

– Rebuilt site or purchased one.

11.3.2. RTO of about 1 or 2 weeks

This RTO allows for staff to be relocated to another site or building with some preparation and installation already done. For example it could be one or more of the following:

– Adapt building from other uses with displacement of staff or budge up activities with making sure that the displaced or budged up activities do not become a problem in the end (backlog).

– Commercial recovery site already contracted with a third-party.

– Prefabricated buildings or mobile units for limited number of people and small unit. This requires substantial preparation like foundations for the prefab.

– Contracted offices that are fully furnished.

11.3.3. RTO of about 1 to 2 days

This RTO allows for staff to be relocated to another site or buildings with some preparation and installation already done. For example it could be one or more of the following:

– Recovery site owned by the organization or another organization (reciprocal agreements with it) in the Commission.

– Budge up: use of existing organization accommodation (e.g. training facility, sport centre) as recovery space or extension of offices. This is only possible if it is carefully planned and after technical preparation.

– Displacement of less urgent activities. Again this requires planning and technical preparation in addition to making sure that the displaced activity does not lead to another serious backlog.

– Remote working, either from home or from another location outside the organization (e.g. hotel, motel). This is possible if there is enough dial-up capacity and if Health and Safety issues are addressed (mainly for working from home).

– Use of a commercial recovery site on a dedicated or syndicated space basis. However, syndication contract should ensure reasonable site availability within 6 hours maximum.

– Use of mobile facilities provided that careful planning and technical preparation are done. Only possible for limited space requirements.

– Contract for managed offices with required processes and staff in place.

11.3.4. RTO of hours or less than a day

An RTO of less than a day will require that the function can be taken on by staff at another location implying the rapid availability of the resources required by that function at the other site, including current information.

– Dedicated site for recovery with rapid availability for staff being redeployed from other tasks. This site can be 'owned' by the organization or made available by another organization in the Commission.

– Relocation of small team of staff to a commercial recovery site that has been contracted on a 'dedicated' basis.

11.3.5. RTO of 'almost immediately'

Like functions with an RTO of hours an RTO of 'almost immediately' will require that the function can be taken on by staff at another location or several locations with a very short notice, implying the 'almost immediately' availability of the resources required by that function at the other site, including current information.

– These recovery locations are, either owned by the organization, or made available by another organization in the Commission.

– Staff and other resources must be ready to take on the tasks with very short notice.

– This requires a 'resilient operation' (dual-site operations and continuous availability solutions).

– In addition, in order to be a viable recovery strategy, this configuration should have no single point of failure and an appropriate geographical separation and diversity of the two or more sites.

11.3.6. Additional tips and remarks

– The choice of the recovery site should be such that staff is willing and able to travel the distance, after consideration of the problems possibly caused by the incident.

– The choice of the recovery site must not be so close that it is likely to be affected by the same incident. It must be beyond the disaster radius.

– The strategy could require multiple recovery sites, either because the number of staff to relocate is large, or because different activities are better recovered at different specialised sites.

– The choice of recovery sites provided by another organization within the Commission or a third-party has to be submitted to contractual or reciprocal agreements that ensure that the required RTO and other service levels are guaranteed:

    – Reciprocal agreements can work between 2 DGs providing each other recovery sites within their own premises, but care must be taken when establishing this type of agreements. For example, periodic checks must be contractually allowed to ensure that the required arrangements have not been changed.

    – Third-party recovery site arrangements from a commercial or Service Company can be an option. As indicated above there are a range of commercial services including fixed, mobile and prefabricated sites.

– The use of recovery sites provided by another organization within the Commission or a third-party has to be supported by a clear statement in contractual agreements as to whether the premises are for the sole use of the organization. In case the recovery premises are shared (syndicated) with other organizations, a plan to mitigate the non-availability of these premises should be devised and documented.

    – Dedicated site is a work area where the organization has exclusive use of accommodation; this is generally used where a rapid RTO ('hours' or 'almost immediately') is required or where the non-availability issue of shared (syndicated) space is judged unacceptable.

    – Syndicated (subscriber) site is a work area where a subscriber pays for the use of accommodation provided that it is not already in use by a prior allocation to another subscriber, so:

        – The maximum number of potential subscribers for a same recovery site that is acceptable to the organization has to be clearly defined in a contract and in the strategy.

- The way space is allocated to subscribers has to be defined in the contract: first come first serve or equitable share (proportion to the resources initially subscribed).

- In case of syndicated space it is important to consider the non-negligible time (1 to 2 days) for a large number of staff to become productive at the site.

- The exclusion zone, which is the distance within which the syndicated resources will not be resold to another potential customer, should be clearly defined in the strategy and in the contract. This exclusion zone depends on the incident type and is the zone potentially impacted such an incident.

11.4. Supporting technologies: Services provided within the organization

11.4.1. Introduction

The often complex strategies for the recovery of information technology services depend on the technology employed and on the previously-defined RTO of the critical functions they support. Typically they will be one or a combination of the following:

- Technology services provided within, and by the organization, which is covered in this section.

- Technology services delivered to the organization by another organization of the Commission (typically DIGIT), which is covered in section 11.7.

- Technology services provided externally by a third party, which is covered in section 11.8.

11.4.2. Approach and strategy alternatives

The first step is to determine a global Recovery Time Objective for the Information Services which must be smaller than the RTO of the supported critical functions.

To simplify the problem we need to break down the supporting technologies into 3 Information System (IS) aspects:

- Data (information):
    - For data recovery, we need to designate off-site storage of copies of data, choose how we are going to back up data on a pre-determined schedule.
    - Sometimes if only data is lost and the system is still operational, the only action required may be recovery of data. So data recovery may be needed not only in the event of a disaster but also when data is lost for other reasons, such as virus, equipment malfunction or accidental mistake.
    - So data recovery is separately covered in section 11.5.
- Information systems (software and hardware), network and communications: based on the RTO need to decide how hardware, software – including communications – will be recovered or replaced in the event of a loss.
- Dependencies with other systems/services, either provided internally, or by another organization/third-party:
    - Need to identify and consider the RTO of other systems that are related to the one we need to recover, so the dependencies currently in place between these systems can be managed and ultimately recovered.
    - This RTO has to be derived from the RTO of the main or dependent system.

The recovery strategies are the alternative ways to recover the group of these 3 IS aspects. The choice of the final strategy has to be done based on a cost benefit analysis or on the potential value of recovery:

- If we must resume certain activities quickly, the recovery strategy should provide resources immediately to substitute for lost resources.
- If some of the activities can wait for recovery, other alternatives can be pursued.
- Generally, the quicker the desired recovery is, the greater the cost of recovery.

The location of critical resources plays a major role in determining effective recovery strategies. In fact the recovery location must not be exposed to the same disaster as the primary location by being beyond the Disaster radius of the disaster.

We can identify different types of alternative 'supporting technology' sites:

- Dedicated sites owned or operated by the organization.
- Reciprocal agreements with an internal or external organization.
- Commercial leased facility.

Regardless of the type of alternative site chosen and based on their operational readiness the three types of alternate sites can be broken down into the following categories: Mirrored site, Hot site, Cold site and Warm site. They are described below. Then two sub-sections are dedicated to alternatives named 'Reciprocal agreements' and 'Co-locations'

Mirrored sites

- They are fully redundant facilities with full and real-time information replication. They are perfect replica of the primary sites from technical point of view. These sites have the highest level of availability as the data is processed and stored at the primary and secondary sites simultaneously (see synchronous replication) or with a slight delay (see asynchronous replication).

- Typically these sites are dedicated sites built, operated and maintained by the organization.

- This is the most expensive solution to maintain and their value is in the recovery of the most critical processes if the business cannot afford any downtime:

    - Certainly required for RTO of 'almost immediately'.

    - Can be advised for RTO of hours or less than a day if allowed by budget.

Hot sites

- It is a fully operational replica of the primary site containing the hardware and system software, supporting infrastructure and support personnel. The only effort for the support staff is to prepare the system to the hot site to begin operations.

- Maintaining hot sites is less expensive than a mirrored site but more than the other types of site, and duplication increases in expense according to the degree of technology duplication and if some asynchronous replication can be done.

- Their value is in the recovery of the most critical processes if the business cannot afford any downtime:

    - Can be used for RTO of hours or less than a day, depending on the time to prepare the system and the way to recover the data (see next section).

    - Is probably not fit for RTO of 'almost immediately'.

    - Can be advised for RTO in the minutes range if staff is ready.

    - Can be advised for RTO of more than a day if the budget allows it.

- An alternative to this strategy is to share the hot site with another organization (DG or family of DGs) if their prime sites are similar enough, with the additional problem that they should not need the site at the same time for their own recovery.

Cold sites

- Have the infrastructure (electrical and physical components of a computer facility) at the recovery site but does not have the computer equipment (it is similar to a second home with supply lines for all utilities, but very little else: inhabitants would need to bring in new furniture and appliances, groceries, pots and pans, and clothes).

- The missing elements must be delivered or moved to the cold site. The recovery time is dependent on the amount of elements to move or deliver to the site, and the time required to 'start' the site (after the staff has moved). Two main solutions:

    - Either the missing elements are available in stock or the like, and ready to be moved to the site. This can speed up the recovery time and be less risky, but can be more expensive than the 'ship-in contract'. It is a strategy possible for RTO in the range of weeks.

    - Or ('ship in contracts') the missing elements (this can include generators, IT equipment such as PCs, servers and printers and specialist hardware such as telephony systems) would be delivered to the site when needed. The delivery time and other required service levels must be ensured by formal contract agreements as contract terms usually vary from best effort to guaranteed delivery. This strategy is appropriate if an unprepared building is to be equipped to provide an appropriate working environment, hence for RTO in the range of months rather than a couple of weeks.

    - The decision as to whether to contract hardware in advance or acquire post-incident must take into account the expected lead-time for acquiring the items in a widespread incident that may be long when less-prepared organizations may be chasing the same equipment.

- An option to this strategy is to share the infrastructure with another organization (DG or family of DGs), with the additional problem that they should not need the site for their own recovery at the same time.

Warm sites

- This is a compromise between hot and cold sites: in addition to the infrastructure, it may include additional resources, such as most commonly used hardware or operating systems.

- Would take longer to prepare for recovery than a hot site but less time than a cold site. The missing elements need to be moved to the warm site using one of the two main solutions described in the cold site section above.

- This strategy would be appropriate for RTO in the range of one week or two, depending on the amount of equipment to move and the way used to recover data.

– An option to this strategy is to share the warm site with another organization (DG or family of DGs) if their prime sites are similar enough, with the additional problem that they should not need the site for their own recovery at the same time.

Reciprocal agreements

– Different organizations (e.g. DG's) within a same family (family of DG's) with comparable needs to support functions, activities or processes could have reciprocal contractual agreements ensuring that an organization could use a site in the other organization to recover its IT in case of problem.

– This strategy seems attractive but the following requirements and caution to consider:

    – First, the two organizations must be in different locations not to suffer from the same disaster or problem.

    – Second, each organization must be willing to help in the event of others need so additional capacity or some sacrifice in data processing needs will arise for the rescuing organization.

    – Third, each organization could modify its processes and systems over time, leading to incompatible processing environment.

    – Finally the contractual agreements must not be too loose such that they are not enforceable.

– This strategy could be appropriate for RTO from a few days up in the best case. This depends on the reciprocal agreements and the distance between the two organizations.

Co-locations

– This is similar to 'reciprocal agreements' but within a particular DG which has information processing facilities in more than one location (e.g. in Brussels and Luxemburg) that are similar in configuration.

– Same challenges as reciprocal agreements that are across DGs:

    – First the two locations must be distant enough not to suffer from the same disaster or problem. If the disaster is a fire in a building, this distance can be short while this distance can be hundreds kilometres in case of an earthquake.

    – Second, each location management must be willing to help in the event of others need; hence the systems, networks, and storage at each site should be sized to cope with the combined traffic and work of the other(s) in addition to its own work.

    – Third, each location should not modify its processes and systems to avoid getting over time a processing environment incompatible with the other location.

  - Finally, the formal agreements between the location management must not be too loose such that they are not enforceable.

- Like for 'reciprocal agreements', this strategy could be appropriate for RTO from a few days up in the best case. This depends on the reciprocal agreements and the distance between the two organizations.

Additional tips and remarks

- Whatever option to replicate the system environment is chosen, current data and copies of software to process the data are needed. So the assessment of the recovery strategies need to take into account the time and cost to restore the data and to install the software where applicable (see next section on data/information).

- To decrease the cost of recovery sites, it is useful to consider holding older equipment as emergency replacement of spares instead of up-to-date ones (possible alternative in some cases).

- Specific strategies ought to be developed to safeguard, replace or restore specialised or custom built technologies with long lead time.

- Remote access: an alternative strategy to relocating people to the recovery site is to provide them with virtual remote access to IT, or though the Internet using Virtual Private Network (VPN) or similar technology.

- Manual versus automation: consideration should also be given to the possibility to fall back to manual procedures to allow for a quicker restarting of the activities in degraded mode.

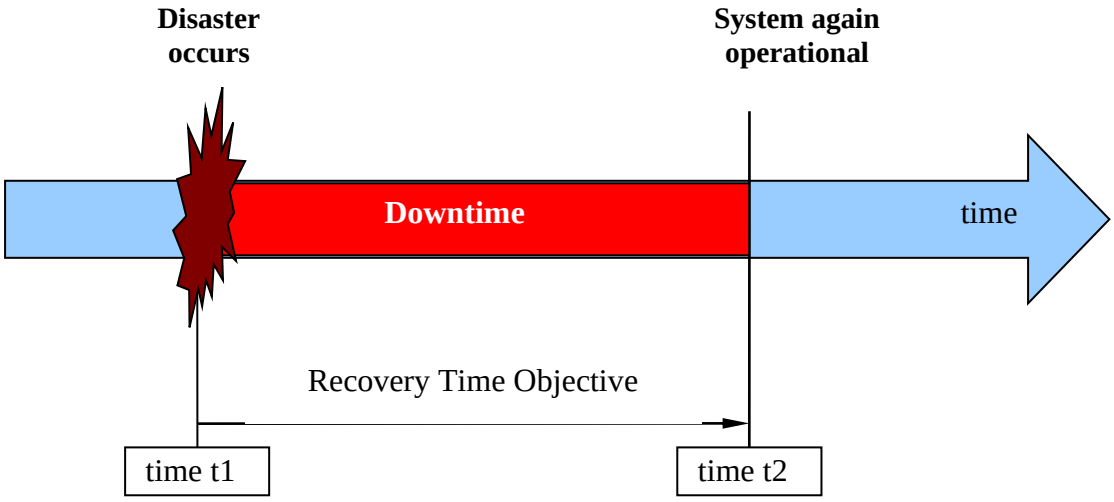
11.5. Strategy for information/data

11.5.1. Important parameters: RTO and RPO

Information continuity strategy has to cover the recovery and availability of the information that is necessary to achieve the RTO of the functions or sub-functions.

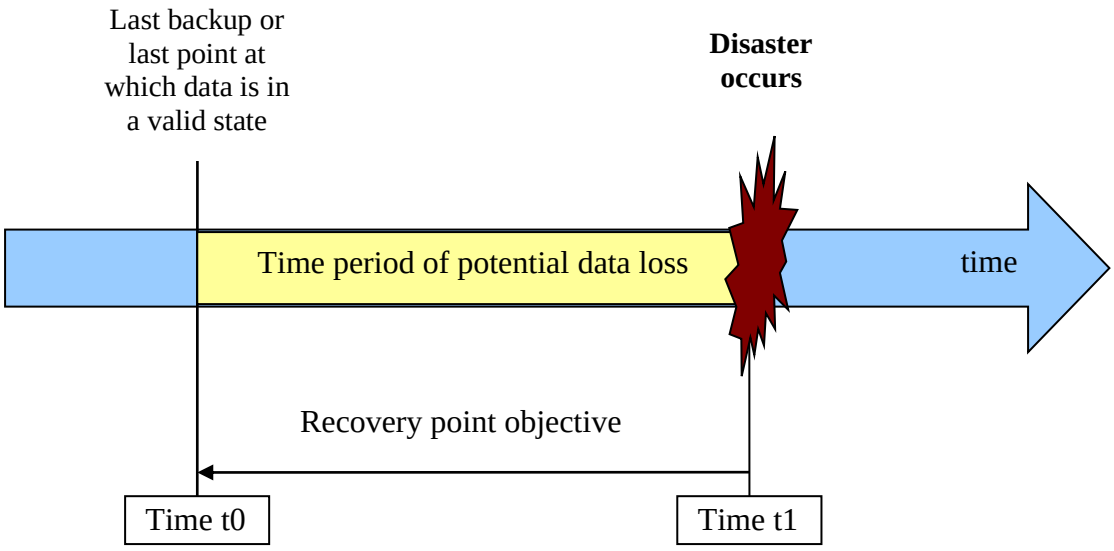
This continuity strategy needs to be defined for each IT resource based on 2 parameters: Recovery Time Objective and Recovery Point Objective.

After the system is ready at a recovery site, the total RTO must take into account the time to get the backup copy of the data and to reload it on the system. (see figure below on recovery time objective). The selection of the backup method has an influence on the time to restore: you must strike a balance between the duration of your backups and the duration of effort for a complete restore.



The other parameter, the Recovery Point Objective, is defined by the approved level of currency of the backed-up data used for recovery after a disaster, so it determines the level of currency of the data after a disaster. See the following picture. If the last backup is done at time t0 and a disaster occurs at time t1, the data processed over the period t1-t0 is lost. In fact after the system is ready, we can only reload the backup of time t0 and need to repeat the processing from t0.

The recovery point objective is what the management has decided to accept as data loss after a disaster. The backup frequency must be set accordingly.



11.5.2. Backup method and currency of the data

There are several technology categories to backup data with different levels of maximum data loss, i.e. different RPO. These technology categories are also characterised by the maximum distances between the primary and secondary sites, as explained below.

Synchronous replication

– In case of synchronous replication between a primary and a secondary site, data arrives at the secondary site as soon as it is written to the primary centre. The processing is hung up at the primary until the secondary site has acknowledged that the data is safely stored at the secondary, hence a performance penalty.

– Except exceptional circumstances at the secondary site there is zero data loss.

– The theoretical distance is 200km but, due to delays and performance, a more sensible distance seems to be around 50km. This also depends on the amount of data and the network type (bandwidth, protocol efficiency).

Asynchronous replication

– With asynchronous replication, the data is copied to the secondary site with some delay, usually less than a minute. So at best only less than a minute worth of data can be lost if a disaster occurs at the primary site.

– No need for acknowledgement back, hence no performance degradation. So there is no limit for the distance between the primary and secondary sites.

Periodic or batch replication

– In this case the data is sent from time to time in batch from the primary to the secondary. This means that the secondary could be hours late at least if not days.

– There is no distance problem. Only the replication frequency and its impact on the primary performance have to be considered for the determination of the RPO.

– Batch replication can be advised if the RPO is 1/2day and above.

Tape backup:

– Backup is regularly taken using tapes and then securely sent to a backup site close to the recovery site. An alternative is to send the data via a network and store the data remotely on tapes.

– As the backups are not taken continuously, the currency of the data is defined by the periodicity of the backup. It is usually taken once a day, so on the average the data would be half a day out of date.

– However if the tapes are not shipped daily to the back up site, the data loss could be considerably higher than 1 day.

– Tape backup can be advised if the RPO is 1/2 day and above.

Important remark on requirements for tape backup

– It is possible that any other replication goes wrong (corrupted files, secondary within the disaster radius). In this case a tape backup would be the ultimate protection against a full loss of data. It is clear that the currency of the data will not be the same but better fairly out of date data than no data at all.

– So, it is highly recommended have a tape backup in addition to other technique for systems that are very critical.

11.5.3. Considerations on restores

The total time to recover a system can be broken down in several parts and the time necessary to restore the data is one of these parts. So during recovery it is essential to minimize this restore time to match the target RTO.

The backup or replication method has a direct effect on the restore speed. Synchronous and asynchronous replications allow the fastest restore. Tape backup gives the longest time to restore: moving the tapes to the recovery site, mount them and restore.

Within some methods like tape or batch replication there are several ways to do the backup: for example full, incremental, cumulative incremental, differential or logging. These ways also have a direct effect on the restore speed: decreasing backup time usually increases restore time.

So you must find a trade-off between backup and restore speeds. Usually the backup process is designed to minimise backup times, but increasing your backup speeds usually slows down the restores. Some examples:

– Logging incremental (daily) changes minimises back-up time;

– Differential (changes since last full back-up) takes longer to back-up but it is quicker to restore.

In case of backup tapes it is important to keep the backup tapes easily accessible and to avoid wasting time to carry them to the recovery site before loading them. In addition it is advised to minimize the number of tapes.

11.5.4. Security requirements of backup/restores

General Backup security

Backups are very valuable to an ongoing operation, but they can also represent a significant potential security hole.

Whatever the type of backup is, the backup data and system are valuable Commission assets like the primary data and systems. So they must be protected according to their security classification in terms of confidentiality, integrity and availability, as mandated in the security policies and standards.

This protection must be effective at all applicable times: for example transfer of data through networks, production of backup copies, transport of backups to safe sites,

storage at backup sites, retrieving information from backup sites, restore on recovery systems.

Only authorised people must have access to the backup data and their storage medium.

Backup data travelling networks or LAN must be encrypted according to their classification (see security policies).

Specific requirements for handling backup tapes and data

As backup tapes are the last line of defence against disasters, they are among the most valuable assets the organization has. They must be protected at all times like the crown jewels of the organization. So it should be possible the entire supporting business function to be rebuilt from them.

The goal in handling backup tapes and data is achieving the proper balance between protecting them from inappropriate access and providing easy access for rapid recovery when the tapes are truly needed.

- Restrict physical access to tapes: unauthorised access to the tapes allows read them back anywhere else (it is like giving root access to a Unix system).
- Magnetically erase tapes before they are reused.
- Encrypt backup data through networks when required by its classification. Pay attention that encryption can have a negative impact on performance of backup process and that you have to keep track of encryption keys.
- Do not allow user-initiated restores without authorization: only people authorized to have access to the data (right level of passwords).
- Protect tapes that leave the organization sites:
    - Make sure that tapes are shipped off-site using secure means (e.g. secure courier).
    - Make sure tapes are never accessed by unauthorised people.
    - If necessary bandwidth is available, consider duplicating your tapes across the network (encrypted), rather than physically transporting them.
- The tapes must be stored beyond the disaster radius of the primary site but as close as possible to the secondary site. These tapes should be physically protected in a locked, hidden, waterproof and airtight vault.
- Label every tape: unlabeled tapes may be blank. No easy way to know if it is blank or not, so prone to unfortunate reuse.

11.5.5. Physical (or hardcopy format)

Using the RTO of the supported function, there is a need to define the physical documents and the level of currency (revision) that must be available to ensure the adequate continuity of the function.

This has to include the plans, procedures and other information about the continuity/recovery of the function, activities and processes.

Then the types of copy must be decided: for example photocopies, microfiches, creation of dual copies at the time of production, scanned to be sent to the recovery site.

Finally there is a need to send the copies and store them in a off-site place such that they are not impacted by the same incident and they are available at the recovery site when needed (not threatening the RTO).

Special attention has to be given to the information that has not yet been copied or stored in a safe location.

Important remark: the continuity strategies must ensure that the physical information is handled at any time in line with its classification of integrity and confidentiality as described in the 844 decision and the 3602 decision. At any time includes: production of backup copies, sending to the backup site, storage at this site, retrieve the information from the storage site to the recovery site (if different of the storage site).

11.6. Summary for site, staff and system/data recovery strategies (services provided within the organization)

Based on the preceding sections on premises/worksite and supporting technologies table 1 below lays down the minimum requirements for site and system/data recovery strategies and related staff to be selected for the services that are provided within the organisation.

Each cell gives the minimum requirements for the strategy choice for site, staff availability, data replication and tape backup for a pair of Recovery Point Objective (RPO) and RTO values.

Recovery Time Objective (RTO) of the system has to be such that the RTO of the supported function is met. The possible values are: several months, about 1 or 2 weeks and above, about 1 or 2 days, hours but less than a day, either 'almost immediately' (seconds) or minutes.

Recovery Point Objective (RPO) is defined by the approved level of currency of the backed-up data used for recovery after a disaster. The different values are: of 1 day or more; around ½ day or more, of a few hours but <1/2 day, of a few minutes, no loss at all.

Types of site arrangement: mirrored site (full replica), hot site (operational replica), cold site (infrastructure in place), warm site (infrastructure and some additional resources), reciprocal agreements (between different organisations in the

Commission) and co-locations (same as reciprocal agreements but within a particular DG/services with multiple and similar IT locations).

Staff – the availability of staff that can be: 'on duty' or 'partly on duty' at the recovery site, available quickly (e.g. on-call at the recovery site), identified and ready to move from another location within a set period of time to ensure the RTO; identified but the move to the recovery place organised at the disaster time.

Data backup or data replication method - possible technology categories to back-up or replicate data with different level of data loss (different RPOs): synchronous replication (simultaneous, zero data loss), asynchronous replication (slight delay between primary and secondary), periodic or batch replication, tape backup.

Tape backup requirement: whether the backup of data using tapes is mandatory or advisable in addition to another method of data replication. In case any other data replication goes wrong (corrupted files, secondary within the disaster radius), tape backup would be the ultimate protection against a full loss of data: the freshness of the data is not the same but better fairly out of date data than complete data loss.

Remark on high availability and disaster recovery:

– Some data replication methods are not suitable for the disasters whose disaster radius is larger than the maximum distance advised for the method. For example for a disaster radius of 100 km, it is not recommended to have a synchronous replication, but an asynchronous one must be chosen instead with some loss in terms of RPO.

– In addition to being suitable for recovery after disaster beyond the disaster radius, the replication methods, which are also high-availability techniques, are also suitable for small incidents or disaster with shorter radius.

Table 1: Minimum requirements for site and system/data recovery strategies

MINIMUM REQUIREMENTS FOR SITE AND SYSTEM/DATA RECOVERY STRATEGIES					
Recovery Time Objective	**Recovery Point Objective**				
	RPO of 1 day or more	**RPO around 1/2 day or more**	**RPO of a few hours but <1/2day**	**RPO of a few minutes**	**No Loss**
Several months	Site: Cold (or shared)	Site: Cold (or shared)	Site: Cold (or shared)	Site:Shared (or Hot - Dedicated)	Site:Shared (or Hot - Dedicated)
	Staff: Identified	Staff: Identified	Staff: Identified	Staff: partly on duty, partly identif.	Staff: partly on duty
	Data: Tape backup	Data: Tape backup	Data: batch replication (or tape backup)	Data: asynchronous replication	Data: synchronous replic.(ATT: see note 5)
	Tape backup: mandatory	Tape backup: mandatory	Tape backup: advis. if batch replic	Tape backup:mandatory	Tape backup: mandatory
About 1 or 2 weeks and above	Site: Warm (or shared)	Site: Warm (or shared)	Site: Warm (or shared)	Site:Shared (or Hot - Dedicated)	Site:Shared (or Hot - Dedicated)
	Staff: Identified and ready to move	Staff: Identified and ready to move	Staff: Identified and ready to move	Staff: partly on duty, partly identif.	Staff: partly on duty, partly identif.
	Data: batch replication (or tape backup)	Data: batch replication (or tape backup)	Data: batch replication (or tape backup)	Data: asynchronous replication	Data: synchronous replic.(ATT: see note 5)
	Tape backup: advis. if batch replic	Tape backup: advis. if batch replic	Tape backup: advis. if batch replic	Tape backup:mandatory	Tape backup: mandatory
About 1 or 2 days	Site:Shared (or Hot - Dedicated)	Site:Shared (or Hot - Dedicated)	Site:Shared (or Hot - Dedicated)	Site:Shared (or Hot - Dedicated)	Site:Shared (or Hot - Dedicated)
	Staff: Quickly avail.	Staff: Quickly avail.	Staff: partly on duty, quickly avail.	Staff: partly on duty, quickly avail.	Staff: partly on duty, quickly avail.
	Data: batch replication (or tape backup)	Data: batch replication (or tape backup)	Data: batch replication (or asynchronous replication)	Data: asynchronous replication	Data: synchronous replic.(ATT: see note 5)
	Tape backup: advis. if batch replic	Tape backup: advis. if batch replic	Tape backup: mandatory	Tape backup: mandatory	Tape backup: mandatory
Hours but less than a day	Site: Hot - Dedicated	Site: Hot - Dedicated	Site: Hot - Dedicated	Site: Hot - Dedicated	Site: Mirrored - Dedicated
	Staff: partly on duty, quickly avail.	Staff: partly on duty, quickly avail.	Staff: partly on duty, quickly avail.	Staff: partly on duty, quickly avail.	Staff: on duty
	Data: batch replication	Data: batch replication (or asynchronous replication)	Data: asynchronous replication (or batch replication)	Data: asynchronous replication	Data: synchronous replic.(ATT: see note 5)
	Tape backup: mandatory	Tape backup: mandatory	Tape backup: mandatory	Tape backup: mandatory	Tape backup: mandatory
Either almost immediately (seconds) or minutes	Site: Hot (or Mirrored) - Dedicated	Site: Hot (or Mirrored) - Dedicated	Site: Hot (or Mirrored) - Dedicated	Site: Mirrored (Hot) - Dedicated	Site: Mirrored - Dedicated
	Staff: on duty	Staff: on duty	Staff: on duty	Staff: on duty	Staff: on duty
	Data: batch replication	Data: batch replication	Data: asynchronous replication	Data: asynchronous replication	Data: synchronous replic.(ATT: see note 5)
	Tape backup: mandatory	Tape backup: mandatory	Tape backup: mandatory	Tape backup: mandatory	
	(rem: HOT for RTO=minutes)	(rem: HOT for RTO=minutes)	(rem: HOT for RTO=minutes)	(rem: HOT for RTO=minutes)	Tape backup: mandatory

Notes 1 - Site: dedicated means that the secondary site is used exclusively for disaster recovery; shared means either co-located or reciprocal agreements.

2 - Staff: used to indicate the degree of readines of the staff responsible for the recovery at the disaster site

3 - Data: indicates the type of replication that is recommended. A second option is within parenthesis if budget permits.

4 - Tape Backup: has to be done if the other types of replication fails. It the last resort in case of extreme problems.

5 - Synchronous replication only advisable for Disaster Radius less than 50 km; for more than 50 km, asynchronous replication is advised

11.7. Services by another organization of the Commission

The recovery of IT services delivered to the organization by a service provider that is another organization of the Commission (typically DIGIT) must be submitted to formal service level agreements stating the disaster recovery requirements approved by the system owner.

The agreements must state that the organization providing the service ensures that the RTO and RPO for the service recovery will be met in case of disaster or disruption. These agreements must be enforceable.

In a nutshell the organization defines the RTO and RPO they need and the organization providing the service must adopt a recovery and data/backup strategy ensuring that the RTO and RPO will be met in case of problem.

In addition, the agreements have to state that the organization must be allowed to carry out testing.

11.8. Services provided externally by a third party

The recovery of IT services delivered to the organization by a service provider that is a third party must be submitted to formal service level agreements stating the disaster recovery requirements approved by the system owner. It is in addition to the other requirements on outsourcing contracts.

The contractual agreements must state that the third-party providing the service ensures that the RTO and RPO for the service recovery will be met in case of disaster or disruption. These agreements should be enforceable by penalties.

In a nutshell the organization defines the RTO and RPO they need and the third-party providing the service must adopt a recovery strategy and data/backup strategies ensuring that the RTO and RPO are met in case of problem.

In addition, the contract has to state that the organization must be allowed to carry out testing.

11.9. Telephony continuation and redirection

A strategy for redirection of telephony to other locations needs careful attention because such redirection could be impossible during wide-area events if it is not planned beforehand. Most telecommunications operators will provide, for a charge, a range of solutions allowing instantaneous or rapid redirection of calls from one site to one or more alternatives.

In addition, once the telephone calls have been redirected, the way of handling telephone calls during an interruption must be defined.

They are many techniques that can be used to ensure the redirection and the communication during the interruption, for example: broadcast notification to staff and other stakeholders, use of non-geographic numbers, call diversion or mobile switchboard.

11.10. Equipment and supplies

A continuity strategy has to be done for the equipment and supplies that are necessary for the function:

– First identification of these equipment and supplies.

– Determine how quickly they must be available at the recovery site following a disaster to meet the RTO of the function.

– Define the strategies to ensure their required availability.

RTO of 'almost immediately', minutes or hours

The equipment and supplies must be ready at the recovery site.

RTO of a few days

They can be

– at the recovery site ready to be used

– submitted to arrangements with third parties for delivery of stock at short notice

– held at warehouses or shipping sites

RTO of a weeks or months

It is advised to have the major parts of equipment and supplies ready in stock held by the organization or third-party. This is surely the case for the equipment and supplies with long delivery delay. For the others that can be delivered with short notice, the order can be placed after a disaster.

Additional tips and guidelines

- Equipment and supplies for recovery must be beyond the disaster radius, wherever they are stored, within a dedicated site or a third party stock.
- The suppliers must not be affected by the same disaster and they must not have too many customers impacted by the same disaster.
- To minimize cost, older equipment can be held as emergency replacement or for spares in a stock beyond the disaster circle (possible solution in some cases).
- Special measures must be taken for the supplies that degrade or evolves over time such that they are rotated with the primary stock.
- Similarly the equipment must stay compatible with requirements (new version) and stay in working order.
- Specific risk mitigation strategies for unique or long lead-time equipment – where possible outdated equipment should be replaced otherwise its updated replacement may threaten recovery time.

- It is important to minimize the risk of supply disruption for the most critical functions by using one of the following techniques:
  - Increasing the number of suppliers.
  - Requiring suppliers to have a validated business continuity capability that you are allowed to test.
  - Holding inventories off-site – at another site or at supplier's site.
  - Significant penalty clauses on supply contracts (though this will not protect against bankruptcy).
  - Identification and pre-acceptance of alternative suppliers.

11.11. Human welfare

There is no point to have excellent continuity strategies without considering the most important asset which is staff.

The organization must define a continuity strategy that takes into account the welfare or their employees, contractors, visitors and customers during an incident and the recovery phase. This is often legally enforced and important for the staff morale and willingness to cooperate.

The best practices require the following issues to be considered:

- Special needs of individuals during evacuations or at the recovery sites like pregnancy, disabilities and family responsibilities.
- During an incident one or more individuals (to be identified in the plans) have to assume responsibility for the following, when applicable:
  - Site evacuation.
  - Accounting for staff, contractors and visitors.
  - Communicating with staff and others on the site.
  - Contact with emergency contact.
  - Translation services.
  - Transport assistance.
  - Setting up a staff help line.
- After the incident there may be additional needs from staff:
  - Temporary accommodation.

  - Counselling and rehabilitation services.

- Welfare needs at alternative locations
  - Refreshments.
  - Personal safety and security.
  - Transport and accessibility.
- Appropriate training on replacement equipment.

11.12. Emergency service liaison

Liaison with emergency local responder has to done early in the definition of BCM strategy to get a clear idea on their tasks of anticipation, assessment, prevention, preparation, response and recovery activities in relation to civil emergencies occurring within their communities.

Interactions with civil emergencies have to be considered in the strategy that should identify the following minimum:

- Staff with an appropriate level of experience and authority should be identified to liaise with the emergency services when they arrive on site in case of problem and subsequently as required.
- The emergency services have to receive information on the location of any casualties and the status of the situations and any known hazards they may encounter.
- During intervention on the disaster site, the emergency services instructions always take precedence over those given by the organization's own staff.
- On their departure from the site, the organization will resume responsibility for its own site security.

11.13. Resource consolidation amongst all key functions

This consists in consolidating the resource requirements derived from the strategy choices done previously for each function.

12. DEVELOPING AND IMPLEMENTING A BCM RESPONSE

In line with the BCM strategies, each organization has to develop and implement various workable and actionable continuity plans describing what to do:

– First to ensure the continuity of critical and essential functions at a recovery site in case of a disaster.

– Then to resume all activities at the main site (or an alternate site if the main is completely destroyed). IT resources recovery is part of these plans.

Timeline of incident/disaster

These continuity plans have to cover the processes and actions necessary from the incident/disaster detection to the complete resumption of all activities.

Usually these plans are expected to consider the following phases:

– Phase one or initial reaction to the incident: escalation to crisis status and damage containment, casualty management.

– Phase two or damages contained: mobilising alternative resources.

– Phase three or resumption beginning: managing alternative resources and resumption of critical and essential functions in order of priority at the primary site (or alternate site if the primary is destroyed).

– Phase four or consolidation: resumption of additional functions at the primary or alternate site.

Plans

There are three types of plans related to the level of people involved:

– Strategic level – Incident or crisis management plan: defines the immediate actions after the incident, the communications plan and more generally how the incident crisis issues are managed by the executive, including the invocation of the other continuity or recovery plans and related teams. If identifiable the trigger elements that will make the executive decide to go (or not to go) into crisis mode has to be defined for each function and identifiable disaster: for example if the incident duration already exceeds a tenth of the MTPD of the function.

– Tactical level – Business resumption plans and disaster recovery plans: addresses the procedures and processes for the teams responsible for the business continuity and resources recovery within the RTO, including IT resources. It has to cover the continuity of essential and critical functions at the recovery site and ensure the resumption of the main site (or an alternative site if the main one is destroyed).

– Operational level – Activity response plans: provides the actions of each business unit of the organization within the overall business continuity plan.

Plans invocation

The method by which each continuity plan described above has to be invoked must be clearly documented. The organization has to describe the instructions and set of criteria defining which individuals are responsible to invoke a plan and under which circumstances.

More specifically the criteria and/or circumstances leading to the declaration of a crisis have to be identified based on an existing formal incident reporting or the occurrence of external disruptive event or disasters.

Plans contents

These plans have to contain the following information:

– Purpose: in terms of targeted functions, their RTO and RPO, level of recovery and conditions of plan use.

– Roles and responsibilities from individual and team perspective.

– Plan invocation and mobilisation instructions: criteria and method of its invocation, team mobilization and meeting point.

– Document ownership and version control.

– Up-to-date contact details for all person Contact details of stakeholders.

– Action plans, task list and resources.

For guidelines and information to develop plans, see the SG document 'Guidance on how to prepare a business continuity plan Version 2 – 10 July 2006' and the 'Good Practices Guidelines of the Business Continuity Institute'.

13. BCM TRAINING AND AWARENESS

Each organization must have an ongoing education and information programme to enhance and maintain the BCM awareness of all staff.

In addition specific BCM training has to be delivered to all staff involved, either in the BCM management and definition, or in incident response or business recovery.

14. TYPES AND METHODS OF EXERCISING BCM PLANS

This section describes the different types of BCM exercises with periodicity of the tests advised by the good practises. Each organization has to define its own testing plan and timetable, depending on their requirements.

14.1. Desktop check

– Check the contents of the plans, either review and update or by challenging the contents.

– Recommended periodicity: at least annually.

14.2. Desktop walk-through

– Extended desk check to check the interactions and roles of all participants

– Recommended periodicity: annually.

14.3. Simulation

– Based on an artificial situation to make sure that the BCM plans contain the information and documentation (e.g. if relevant: building plans, communications) required to carry out successful recoveries.

– Recommended periodicity: annually or less.

14.4. Function(s) testing

– Exercise the moving of work to the alternate site involving all parties: relevant employees, site suppliers, other external parties. This needs to be done without jeopardising the business as usual.

– Recommended periodicity: annually or less.

14.5. Limited scenario test

– Similar to function testing but on a limited scope, like testing the recovery of an IT system, or the escalation and call-out communications.

– Recommended periodicity: at least annually or twice yearly.

14.6. Full test

– Very complex testing that implies testing the full BCP and incident management. This can implies shutting down an entire building or set of buildings and relocating work at the alternate site. This should not jeopardize the business as usual.

– Recommended periodicity: annually or less.

15. EXERCISING, MAINTENANCE AND AUDIT

15.1. Realistic and robust exercising

Each organization must set up a structured testing programme for BCM ensuring realistic, robust and carefully planned exercising of all BCM plans. A timetable must be devised such that all relevant personnel are included in the exercise activity and all technical, logistical, procedural, administrative and operational aspects of the plans.

These exercises must be prepared with extreme care to ensure minimum risk to existing business processes.

The organization must plan the different types of exercises regularly (at least one a year) and when it is necessary after changes in the plans.

15.2. Exercising outsourced function or services

As the outsourcing organization is always fully accountable for the outsourced function or services, it has to require in a contract and under SLAs that the supplier organization provides evidence of viable continuity plans and results of their exercising. This has to be done for suppliers that are other organizations in the Commission or third-parties.

15.3. Maintenance and review

The organization must establish a maintenance programme to ensure that any internal or external changes to the organization business objectives, functions, dependent activities and supporting resources are reviewed in relation to BCM.

At least annually the BCM arrangements must be reviewed to make sure they are still adequate and effective.

15.4. Audit and self-assessment

The BCM capability and processes must be regularly submitted to independent audit, either external or internal. Audit findings must be considered in a formal BCM review process.

A self-assessment process for BCM capability against the organization objectives and relevant good practices has to be included in the BCM review.

16. REFERENCES

SG: Framework for Business continuity management in the Commission – SEC(2006)898

BS 25999-1:2006 – Business continuity management – Part 1: Code of practice

Guidance on how to prepare a business continuity plan Version 2 – 10 July 2006

Standard on Risk Management – version 01.10

Business continuity of ICT infrastructure services ensures public value. Marcel Jortay (Directeur DIGIT C) - Bulletin Informatique nr 3/2007

IT facilities and business continuity – Michael Sonderskov and Thomas Michlmayer Digit C2 –Bulletin Informatique nr 3/2007

The IT foundation for business continuity @ DIGIT - Thomas Michlmayer Digit C2 and Tom Vekemans (DIGIT C1) – Bulletin Informatique nr 3/2007

Mise en place d'un Disaster Recovery Plan grâce à la "virtualisation" – Yves Dubocquet (Trade). - Bulletin Informatique nr 3/2007

Business Continuity Institute - Good Practices Guidelines

17. RELATED STANDARDS AND SUPPORTING GUIDELINES

Standard on Business Continuity Management

Standard on Risk Management

18. APPENDIX 1: FUNCTION OR PROCESS MAPPING

As a reminder to be in line with the Secretary General "Framework for Business Continuity Management in the Commission" the term function is used as a generic term for activities, processes, services and infrastructures.

We can also define activity as the process or set of processes that are implemented in an organization to produce or support one or more products or services.

Functions depend on the existence or availability of supporting resources like facilities, buildings, IT infrastructure (including voice and data communications), hardware and software, vital records, data, business partners and staff.

Functions can also depend on other sub-functions that in turn depend on supporting resources.

Before deciding on the priorities for recovery there is a need to first identify the mission-critical functions derived from the business objectives. This will be done at different levels in the organization of the Commission:

- Either within each DG or family of DG's (e.g., HR.DS family)
- Or at the Commission level which will be referred to as Secretariat General level

One function in one DG can be dependent on one function or on one of its components in another DG. So it is important to identify the dependability of functions on others, wherever they are anchored, either in the same DG or in another one.

Similarly the dependability on functions provided externally to the Commission also needs taking into account in the identification of the components of mission-critical activities.

The function (or process) mapping technique can be used to analyze the inter-relationships and operation of the overall function, super-functions, functions and sub-functions. This activity map gives a top-down view and thorough understanding of the business organization of a DG, family of DGs or the Commission (via the SG).

The figure A1 shows an example of a generic function map with four levels:

- Overall function - for example it could be HR.DS DG overall process.
- Super functions - for example HR.DS DG overall process split in 5 super activities: Crisis management team super-process, Security directorate, Directorate A process, Directorate B process, Directorate C process.
- Functions – for example the Crisis management team super-process (Super-function 1) could be split into the 4 following activities:
  - (Function 11) Coordinate with the commission-level crisis committee
  - (Function 12) Dealing with the media
  - (Function 13) Manage the crisis response to the crisis at all levels
  - (Function 14) Briefing of HR.DS staff

- Sub-functions – for example the function 12 could be split into 2 sub-functions or tasks:
  - (Sub-function 121) Provide the line-to-take to the spokesperson
  - (Sub-function 122) Ensure coherence with dealings with the media.

Such a function map allows understanding how an organization (DGs of family of DGs) conducts its operation. By drilling down from the overall function to individual tasks, it is possible to identify the functions that are mission-critical and/or time-critical and their supporting resources like for example staff, facilities and systems. They allow determining the single points of failure and visualizing the business needs for continuity.

In addition the process and overall function approach should also help determine the inter-dependency across DGs and dependency on external service providers.

A standard naming convention should also be adopted to enforce consistency and facilitate not only communications to management but also throughout the whole process of business continuity planning, from the writing of plans to testing and maintenance.

The number of business functions should be limited to a workable number in order to be efficient: first limit the number of overall activities and then the number in other levels from 8 to 12. Fewer levels are even better if it is sufficient for the business understanding.

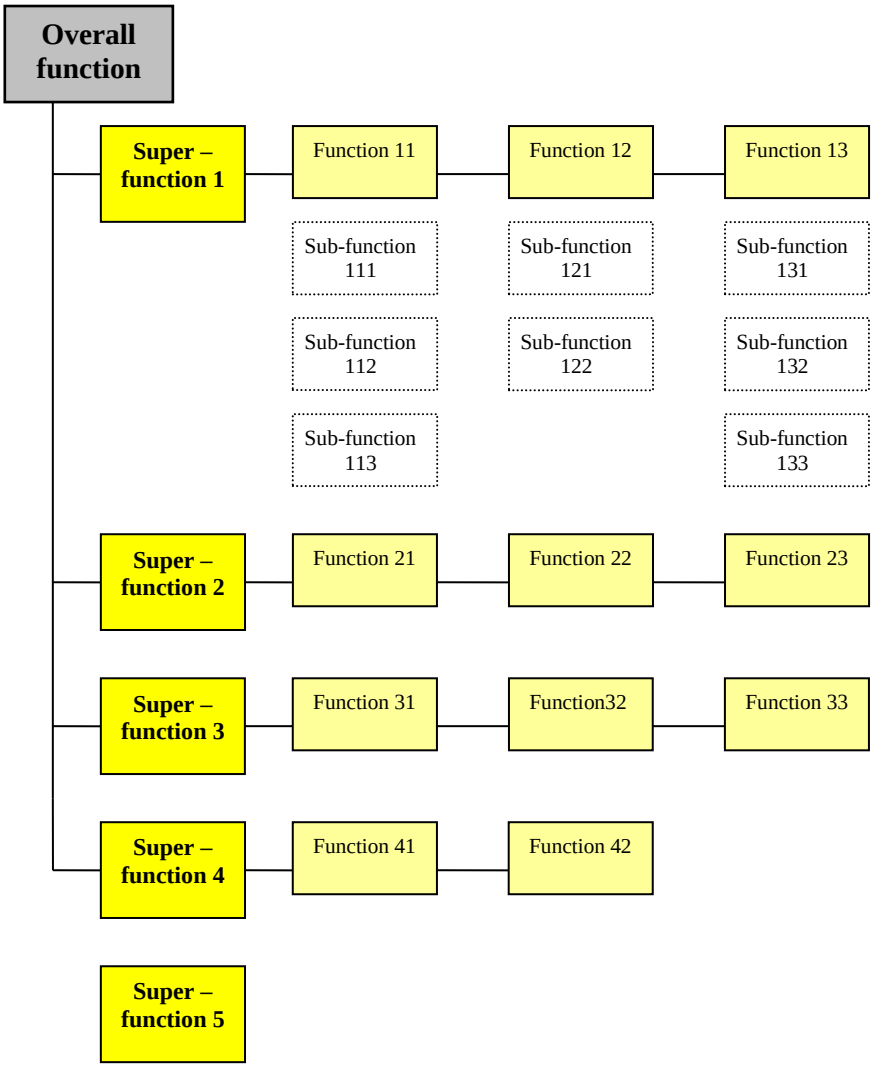


Figure A1: Example of detailed function map

19. APPENDIX 2: TOOL TO ASSESS THE CRITICALITY OF A FUNCTION (WITH EXAMPLE)

Business continuity management scope					
Questionnaire for function criticality					
	Questions	**Weight**	**Answer**	**Value**	**Notes**
1	Does this function support a business objective of your organization?	10	1	10	1=yes, 0=No
2	Is this function performed only by your organization, or is it also performed by other organizations within the Commission?	5	0	0	1=only own org 0=other orgs
3	Does another organization, vendor, partner, government or external organization depend on this function or successful completion of its function?	7	0	0	1=yes, 0=No
4	Is there a potential either for loss of reputation or adverse publicity or for political problems?	10	0	0	1=yes, 0=No
5	Is there a potential for loss of life or injury to personnel, business associates, or externals if this function is not carried out?	10	0	0	1=yes, 0=No
6	Is there a potential for significant financial loss to the organization if this function is not carried out?	7	1	7	1=yes, 0=No
7	Is there a potential for significant fines, litigation, jail terms, or other punishment for non-compliance to a required regulatory or contractual requirement?	7	0	0	1=yes, 0=No
8	Is non-compliance tied to a specific threshold for downtime of this function?	5	0	0	1=yes, 0=No
9	Is non-compliance tied to a specific for data loss or disclosure of sensitive information for this function?	3	0	0	1=yes, 0=No
10	Is this function carried out by key (critical) personnel within the organization?	10	1	10	1=yes, 0=No
11	Are other personnel within the organization available and capable of performing the function in the absence of key personnel?	5	0	0	1=yes, 0=No
12	What priority would your organization give this function within the entire Commission?	10	2	3	5= very high, 4=High,3=Medium,2 =Low, 1=very low
13	Is it a perceived high-risk location (due to the proximity to potentially dangerous industrial area or prone to physical threat like flooding)	7	1	7	1=yes, 0=No
	Totals	96		37	
	Score in %	**39%**		In scope for BCM if score >=30%	

Notes:

It is possible to customize the table to reflect the reality of the organisation.

It is possible to change the weight given to each question and it is also possible to add or withdraw questions.

The threshold above which the activity is advised to be included in the BCM can also be adapted.

20. APPENDIX 3: FORMAL METHOD FOR BUSINESS IMPACT ASSESSMENT FOR BCM

20.1. Principles

It consists in determining the possible business impacts resulting of major incidents or disasters from availability of the function or activity perspective.

It consists in scoring the business impact of some disasters or major incidents occurring with the following principles in mind.

- Assume worst-case disaster scenario (day of week, month of year, etc): for example for assessing the Maximum Tolerable Period of Disruption of seasonal or periodic functions, focus impact analysis on interruption during one peak
- Assume no countermeasures in place and more specifically no recovery capability exists
- Obtain raw number in order of magnitudes instead of wasting effort in hunting unnecessary accuracy
- Validate BIA data with all BIA participants
- Formalize decision from Director General so lower-level management (MTPD timeframes, scope, and depth of recovery procedures, etc) can make precise continuity plans in the following steps described further in this document
- Customize the BIA information-gathering tools questions to suit the organization's customs/culture
- Focus on time-critical business process and support resources (i.e., systems, applications, voice and data networks, facilities, people, etc)

20.2. Tools

20.2.1. Rating levels

The availability ratings are worst case ratings of the business impact or damage resulting from disaster or serious incidents causing interruption of the function. The following ratings or impact levels will be used to measure this impact.

Rating/Impact level	Significance or level of damage
1	Very Low (negligible or no damage)
2	Low (moderate damage)
3	Medium (significant damage)
4	High (serious damage)
5	Very High (from exceptionally grave damage to catastrophic)

20.2.2. Forms

Three documents are available to perform and support the determination of the function classification and MTPD process. These documents are described in the following sections and given in the appendices:

– Business impacts definition table (appendix 4)

– Business impact levels reference table (appendix 5)

– Function MTPD and classification table (appendix 6)

20.2.3. Business impacts definition table

The Business impacts definition table has to be used by the BIA participants to help **identify business impacts relevant to the Commission.** The business impact types have been identified in relation to the business of the Commission and their categories have been derived from the Risk management framework provided by the DG BUDG.

The Business impacts definition table, which is given in appendix 6, contains 2 columns.

The first column defines 15 types of business impacts grouped in the following 4 main categories:

– External environment, which contains 5 impact types (e.g. Damage to Commission's partner)

– Planning, Process and systems, which contains 5 impact types (e.g. Unforeseen or additional costs)

– People related, which contains 3 impact types (Damage staff morale/productivity)

– Legality and regularity aspects, which contains 2 impact types (Legal liability and penalties)

For each business impact type listed in the first column, the second column provides examples of business impacts identified as relevant and/or specific to the Commission. This gives an indication on the kind of impacts that are expected in the related category. It is important to know that they are only examples of business impact and that the list of examples does not pretend to be exhaustive. During a BIA exercise other business impacts that are not in the list for a particular impact type are likely to be identified.

The overall structure of the documents described in the following sections is exactly the same as the Business impacts definition table and mapped on the contents of the first column. In a nutshell they are based on the same business impact types and their main categories.

20.2.4. Business impact levels reference table

The Business impact levels reference table has to be used to **help determine the ratings during the assessment of the function interruption impact values**. The Business impacts levels reference table, which is given in appendix 5, contains 7 columns.

The first column is the same as the first column of the Business impacts definition table and provides the 15 impact types grouped in the same four categories.

For each impact type of the first column, the second column, which is named "Evaluation criteria", provides recommended or proposed measurement types for the rating. For example the Impact type "Damage to commission's partner" can be assessed in two ways:

– Either qualitatively by the "extent of damage".

– Or quantitatively by the estimation of the financial impact proposed as a percentage of a budget. This budget can be the total budget of a particular organization. This total budget can be determined during the BIA process of the BCM.

– The choice between the two depends on the specific business impact that is identified and the information available about it.

For each business impact type of the first column and the measurement criteria of the second column, the following five columns provide a value or range of values for each of the impact levels 1 to 5. The proposed value is quantitative or qualitative depending on the evaluation criteria. Considering the same example "Damage to commission's partner", if the impact identified by the system owner is "Damage the continuing effectiveness of security or intelligence operations" and his qualitative assessment of the damage is "Significant", the table proposes a rating or impact level of 3.

20.2.5. Customization of the business impact levels reference table:

Due to the differences in business and budget in different organizations (DG or DG family), a same cause can have very different levels of business impact. So it can be useful to adapt the Business impact levels reference table to the reality of the organization.

It is recommended to do this customization carefully in order to keep the essence of this method. So, before using the customized table for actual rating in an organization, it should be formally approved by their director(s) general.

The percentages of total budget or range of percentages given can be different in different organizations. The percentages given in the table are proposals that can be customised. It is then advised to review the reference table organization-wise and to get an agreement on the percentages that have to be used consistently for the BIA exercises of the organization.

Another way of customizing the financial impact is to replace the percentage by the calculated values using the actual budget to be considered. For example if the total budget of 1000 million Euros for a programme is used, the impact level 2 (low) will be from 100 KEur to 1 million Euros.

Similarly, this reference table could also be customised in the "extent of delay" evaluation criteria for the "Degraded service" and "Impaired political decision/execution" impact types.

20.2.6. Function MTPD and classification

Availability rating (impacts)

The availability rating is the assessment of the business **impacts** for a specific interruption of the function for each of business impact types. This will be done by filling in a blank Function MTPD and classification table given in appendix 6 with the support of the two tables described above: the Business impacts definition table and the Business impact levels reference table.

The first column of the Function MTPD and classification table contains the same impact types grouped into the same four categories as the first column of the Business impacts definition table. There are two additional rows described further in the section:

– The first one dedicated to the summary of ratings.

– The second one dedicated to the overall assessment of Maximum Tolerable Period of Disruption and function classification

The following five columns are dedicated to get the ratings corresponding to the business impact type of the first column.

It consists in providing a rating of the business consequences (worst case) of function being unavailable for each of the Business impact types corresponding to a row in the table unless the impact type for the function being classified is not relevant and for each of the different duration of interruption (12 hours, 1 day, 2 days, 1 week, 2 weeks) in the row:

– This means that you have to write a number (impact level value) between 1 and 5 in each cell of a row corresponding to an impact type, unless the impact type is not relevant for this function assessment.

– The impact level value will increase with the duration of outage from left to right in the table.

– So this means that only the value 1 can be found to the left of a cell where level value 1 is identified and the value 5 to the right of a cell where level 5 is identified.

For example consider that we are figuring out if an interruption of the function Y could have a business consequence of the type "Damage to image or reputation":

- We look into the Business impacts definition table and we try to figure out if any of the examples given for this type is or are relevant to this situation.

- After discussing various scenarios in their worst case, we realise that the most serious damage in this example would be "Damage to reputation".

- Then we use the Business impact levels reference table at the same row "Damage to image or reputation" and look if we can assess the impact with numbers (financial impact) or only with qualifier (extent of negative publicity). We decide that it is possible to assess with qualifiers.

- So we proceed with the assessment for each duration of interruption and we get to the agreement that the most likely impact value if we consider the worst case would be the following for each duration of outage:

  - 12 hours: the impact is assessed as "negligible or no damage", which corresponds to a level of 1 or Very Low.

  - 1 day: the impact is assessed as "Local negative publicity", which corresponds to a level of 2 or Low

  - 2 days: the impact is still assessed as "Local negative publicity", which corresponds to a level of 2 or Low

  - 1 week: the impact is assessed as "Significant or limited to 5 EU countries", which corresponds to a level of 3 or Medium

  - 2 weeks: the impact is assessed as "Serious or Europe-wide negative publicity", which corresponds to a level of 4 or High

- Finally we report these ratings by writing the values into the cells that are at the intersection of the row "Damage to image or reputation" and respectively each of the column 12 hours, 1 day, 2 days, 1 week and 2 weeks. This will give in our example: 1 for 12 hours, 2 for 1 day and for 2 days, 3 for 1 week and 4 for 2 weeks.

We have to give a rating for each cell in a row corresponding to an impact type relevant for this function assessment.

The last column named "Comments" can be used to refer to the reasoning behind the ratings of the same row. If there is not enough room in the cell, it could be a number referencing a longer explanation in a companion document. It is strongly recommended to document the reasons for the ratings, especially for 4 and 5 ratings. Such reasoning is very useful during future BIA exercises

Finally when all the impact types have been considered and all the ratings reported it is time to summarize the availability ratings in the "Summary of rating" row.

– All the cells of the summary row must be filled in. We need to proceed column by column.

– As the summary has to indicate the highest damage assessed in the rows above, we just need to report in a cell of the summary of rating row the highest rating in all the cells of the column above.

– In our example, we assume to have filled in all the lines and by following the instructions just above we assume that we get the following sequence of values from left to right: 1, 2, 3, 4 and 4 respectively for outages of 12 hours, 1 day, 2 days, 1 week and 2 weeks.

Assessment of MTPD and function classification

Then, it is required to do the overall assessment of the Maximum Tolerable Period of Disruption, i.e. the timescale beyond which a disruption of the function is unacceptable to the business. It is recommended to proceed as follows:

– The "owner" of the function has first to define the level of harm that is unacceptable for the business: in our example he considers it is "Europe-wide negative publicity".

– This unacceptable level of harm "Europe-wide negative publicity" corresponds to a level 4 or "High" in the Business Impact Reference Table.

– Then, in the Summary of ratings that has just been established in the Availability rating form (sequences of values from left to right: 1, 2, 3, 4 and 4 respectively for outages of 12 hours, 1 day, 2 days, 1 week and 2 weeks), level 4 identifies the duration of interruption that corresponds to that level of unacceptable harm: in our example, the duration when the harm becomes 4 is one week.

– So the MTPD that corresponds to the level of interruption unacceptable for the business has to be lower than, or equal to the duration of 1 week, which corresponds to the duration of interruption when the impact level becomes 4.

– In the light of the information above, the various BIA participants get to the agreement endorsed by the "owner" of the function that the MTPD is 3 days.

Finally the actual function classification has to be derived directly from the MTPD defined just above and using the same row as for "Overall assessment of Maximum Tolerable Period and function classification" in the following way:

- If the MTPD is more than 1 week, the resulting function classification is "Necessary"

- If the MTPD is more than or equal to 2 days, but less than or equal to 1 week s, the resulting function classification is "Essential"

- If the MTPD is less than 2 days, the resulting function classification is "Critical"

- Then the final function classification can be reported in the last row by just erasing the classification categories that have not been chosen.

21. APPENDIX 4: BUSINESS IMPACTS DEFINITION TABLE

Business impact types	Examples of types of business impacts
External environment	
Damage to political relations	Intervention at political level (Council, Parliament) about EC's performance Problems in diplomatic relations Problems with friendly / unfriendly government
Impaired political decision/execution	Political decisions and priorities delayed or not taken Aid, subsidies, grants, programs delayed, not executed or missed
Damage to Commission's partner	Damage to Commission partner (member states companies, citizens, contractors, consultants) Damage the operational effectiveness or security of Members states or other contributors force Damage the continuing effectiveness of security or intelligence operations Damage member states financial, monetary and commercial interests Damage the financial viability of major organisations
Damage to reputation/image	Damage to reputation (eg due to disclosure of confidential information, compromised info, info not available)
	Damage to image (due to disclosure of confidential information, compromised info, info not available)
Damage to public order	Cause protest, demonstration or prejudice public, locally or more widespread due to delayed or not executed EC decisions or policies
Planning, processes and systems	
Loss of management control	Impaired decision making Jeopardise the realisation of major policy objectives Impede the development or operation of major EU policies Cause problems on important negotiations involving political damage or financial losses Process management failure Implementation of policies affected by non-reliability of available information Implementation of policies affected by delays in receiving the data
Degraded service	Degraded service provided (for internal customers or external partners) Cause problems to EU management, activities or operations Delayed deliveries (project)
Unforeseen costs	Recovery costs, uninsured losses, increased insurance, Cost to detect the cause of the harm and to repair it
Loss of tangible assets	Material loss or theft Fraud, theft of money, lost interest Loss of EU funds caused by fraud
Budget overrun	Could also lead to Intervention at political level (Council, Parliament) about EC's performance
People related	
Health and safety	Injury or loss of life of staff, suppliers, contractors and others employed by the EC (directly or indirectly)
Damage staff morale/productivity	Distress (=anger, frustration, disappointment, embarrassment or concern) Prejudice individual security or liberty Reduction in staff morale/productivity (reduce efficiency, lost time, job losses)
Fraud or irregularities	
Legality and regularity aspects	
Impede law/rules enforcement	Facilitating commission of a crime, prejudice the investigation of a crime Impede the procedure of selection, fair assessment of readiness of candidates or fair evaluation of experts,
Penalties and legal liabilities	Civil suit or criminal offence resulting in damage/penalty Result in the infringement of laws, regulations and contractual obligations Claims against the commission due to disclosure of confidential information

22. APPENDIX 5: BUSINESS IMPACT LEVELS REFERENCE TABLE

BUSINESS IMPACT LEVELS REFERENCE TABLE						
Business impact types	**Measurement criteria**	**Impact levels**				
		1 Very Low	**2 Low**	**3 Medium**	**4 High**	**5 Very High**
External environment						
Damage to political relations	Extent of damage	Minor or no damage	Moderate	Significant or adversely affect	Serious, raise tension or formal protest	Exceptionally grave
Impaired political decision/execution	Extent of delay (time) or	One week or negligible time	One month or moderate time	Six months or significant delay	One year or serious delays	Exceptionally grave delay or abandoned execution
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Damage to Commission's partner	Extent of damage	Minor or no damage	Moderate	Significant or adversely affect	Serious	Exceptionally grave
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Damage to reputation/image	Extent of negative publicity	Minor	Moderate or local negative publicity	Significant or limited to 5 EU countries	Serious or Europe wide negative publ.	Very serious or worldwide negative publ.
Damage to public order	Extent of damage	Minor or very localised protest	Limited or localised protest	Demonstrations national effects injured people	Widespread effects/ death of 1 individual	Threat stability/ widespread loss of life's
Planning, processes and systems						
Loss of management control	Extent of problem	Minor or no damage	Moderate	Significant or impede important executions	Serious or disrupt important executions	Exceptionally grave or abort critical execution(s)
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Degraded service	Extent of damage	Minor or no damage	Moderate/	Significant/ adversely affect	Serious	Exceptionally grave
	Extent of delay (% of total expected time)	One day or negligible time (1%)	One week or moderate time (10%)	One month or significant delay (25%)	One year or serious delays (50%)	More than one year or 75% or abort project/delivery
	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Unforeseen costs	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Loss of tangible assets	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Budget overrun	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
	Extent of damage	Minor or no damage	Moderate	Significant/ adversely affect	Serious	Exceptionally grave
People related						
Health and safety	Number of incidents & extent of harm	Minor injur(ies)	More than minor injury(ies)	Life of indivdual(s) threatened	Death of one individual	Widespread loss of life
Damage staff morale/productivity	Extent of loss of morale	Minor or no loss	Moderate	Significant	Serious	Complete loss
Fraud or irregularities	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
Legality and regularity aspects						
Impede law/rules enforcement	Extent of damage	Minor or no damage	Moderate	Significant/ adversely affect	Serious	Exceptionally grave
Penalties and legal liabilities	Financial (% of budget)	Less than 0,01%	0,01% to 0,1%	0,1% to 1%	1% to 10%	More than 10%
	Extent of damage	Minor or no damage	Moderate	Significant/ adversely affect	Serious	Exceptionally grave

23. APPENDIX 6: FUNCTION MTPD AND CLASSIFICATION FORM

Business Impact Assessment BCM: FUNCTION MTPD and CLASSIFICATION						
Business impact types Business consequences of a prolonged interruption of a function (worst case)	**Business impact levels** 1=very low, 2=low, 3=medium, 4=high, 5=very high **Duration of interruption**					**Comments**
	12 hours	**1 day**	**2 days**	**1 week**	**2 weeks**	
External environment						
Damage to political relations						
Impaired political decision/execution						
Damage to Commission's partner						
Damage to reputation/image						
Damage to public order						
Planning, processes and systems						
Loss of management control						
Degraded service						
Unforeseen costs						
Loss of tangible assets						
Budget overrun						
People related						
Health and safety						
Damage staff morale/productivity						
Fraud or irregularities						
Legality and regularity aspects						
Impede law/rules enforcement						
Penalties and legal liabilities						
Summary of rating	**12 hours**	**1 day**	**2 days**	**1 week**	**2 weeks**	
What is the most serious impact which would arise from interruption of the function. Tip: this would normally be at least as high as the highest individual rating assessed above.						
Overall assessment of Maximum Tolerable Period of Disruption and function classification						
What is the timescale beyond which the interruption of the function is unacceptable for the business of the Commission?	MTPD = Necessary / Essential / Critical					Legend Necessary: > 1 week Essential: >= 2days but <=1week Critical: < 2days