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

Brussels 28/05/2010
HR.DS ARES (2010)288262

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON BUSINESS CONTINUITY MANAGEMENT

ADOPTED BY MRS. IRÈNE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 28/05/2010

Version 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. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

In line with the SG's 'Framework for Business Continuity Management (BCM) in the Commission' this standard establishes the rules for the Business continuity management at the Commission with an emphasis on Information Systems Security.

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.

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.

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.

2.1. Scope

As indicated in the 'Framework for Business continuity management in the Commission' published by SG {SEC (2006)898}, the scope of this standard 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.

2.2. 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.

2.3. 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.

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.

3. SECURITY CONTROLS

3.1. Policy objectives

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.

3.2. Risks 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. Security Controls statements

(1) The process leading to the definition of the Business Continuity plans and elements related to IT and information systems security must be integrated into the overall Business Continuity Management of the Commission services' important or mission-critical processes, functions and activities supported by the information systems, as stipulated by the Secretariat General's framework.

(2) The BCP strategy for the IT resources (systems, networks, data, applications) supporting the important functions of the Commission services must be defined based on the 3 parameters Recovery Time Objective (RTO), Recovery Point Objective (RPO) and Disaster Radius.

(3) These parameters are related to the business functions that the IT resources support and must be derived according to the overall BCP process recommended by the SG and also described in the Guidelines on Business Continuity Management.

(4) Every business function that is recognized as mission-critical to the business objectives of the Commission services and within the scope of BCM must be submitted to a Business Impact Assessment to determine its Maximum Tolerable Period of Disruption (MTPD) and its category 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.

(5) For each critical or essential function, it is necessary to identify the type, number and inter-dependencies of its supporting resources, infrastructure and other functions that are absolutely required to resume and continue the function at a service level satisfying the organisational objectives within the MTPD.

(6) After a risk assessment considering all the potential disasters and important events threatening the critical and essential functions and their resources in each of their locations, the decision to adopt a BCP strategy or not must be done against these levels. If the instructions of the document Guidelines for Business Continuity Management are followed:

- a BCP strategy must be implemented if the resulting risk level[1] is 'high' or 'significant';
- a BCP strategy can be implemented if the resulting risk level is 'moderate';
- for each location, the "**overall Disaster Radius**" must be defined as the largest disaster radius of all the potential disasters or important events for which a BCP strategy has been decided for the location.

(7) The alternate or recovery site where the IT activities need to be restarted in case of disaster or main disruptive event at the main site must be located beyond the overall disaster radius resulting from the risk assessment.

(8) In addition to the IT hardware and software, all resources necessary to restart and operate the IT activities at the recovery site must not be impacted by the disaster and, hence, must be beyond the overall disaster radius: for example, key staff, stationary, telecoms, backup tapes, backup sites and equipment.

---

[1] See the "Guidelines on Business Continuity Management" for more details on risk calculation and risk strategy determination. The result of risk assessment can lead to 4 levels: high, significant, moderate and low.

(9) Considering that the MTPD is determined as the point at which the organization will just survive when recovering a key activity, one must consider some margin and define a shorter recovery time for this key activity called Recovery Time Objective to take account of unexpected problems during a recovery.

(10) All key resources (including IT resources) that are necessary for the recovery of a key function must be recovered within their own RTO such that the aggregation of the RTO's of all supporting resources allows the overall RTO of the key function to be met.

(11) Specifically the RTO of the IT resources has to be chosen accordingly. Finally the RTO of the IT resources has to be chosen as the minimal of all RTO's respectively derived from each of the key functions they support.

(12) All the other resources necessary for the set-up and recovery of IT resources at the site must be considered in the overall RTO in terms of time to move people, the backup tapes and the material for example.

(13) The frequency of information backup and the high-availability arrangements between the main and recovery sites must comply with the value of the Recovery Point Objective (RPO) of the data approved by the system owner.

(14) The backup data and system must be protected according to their security confidentiality and integrity classification 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.[2]

(15) While or after ensuring the continuity of the chosen critical and essential functions at the recovery site(s), the resumption of the complete set of functions of the organization must be started at the primary site if this one has not been destroyed. In case of its destruction the resumption has to be done at an alternate site, which could be the recovery site.

3.4. Minimum requirements for site and system/data recovery strategies

3.4.1. Services provided within the organisation

The table 1 given below defines the minimum requirements for site, 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 strategic choice for site, staff availability, data replication and tape backup for a pair of Recovery Point Objective (RPO) and RTO values.

---

[2] See Guidelines for Business Continuity Management for indications on security requirements of backup/restores and specific requirements for handling backup tapes and data.

Nevertheless, these minimum requirements could be achieved by other means. Therefore, alternate means could be selected considering it provides an equivalent level of assurance.

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 or 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 within a same family 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 technological categories to back-up or replicate data with different levels 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.

Remarks on high availability and disaster recovery:

- Some data replication methods are not suitable for the disasters whose 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

3.4.2. 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 and derived from table 1.

These requirements must include the RTO and RPO to be ensured by the servicing organisation, the possibility to carry out testing and a justification of the disaster radius.

3.4.3. Services provided externally by a third party

The recovery of IT services provided by a service provider that is a third-party must be submitted to the same requirements as in section 3.4.2 in addition to the other requirements on outsourcing contracts.

4. DEVELOPING AND IMPLEMENTING A BCM RESPONSE

In line with the BCM strategies, each organization has to develop and implement various workable, feasible 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, and
- 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.

These plans must 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 at the recovery site.
- Phase three or resumption beginning: managing alternative resources at the recovery sites 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 must be 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 plans.

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 RTOs and RPOs, 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.

5. BCM TRAINING, AWARENESS, EXERCISING, MAINTENANCE AND AUDIT

(1) Each organisation must have an ongoing education and information programme to enhance and maintain the BCM awareness of all staff.

(2) 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.

(3) Each organisation 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.

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

(5) The organisation must plan the different types of exercises regularly (at least one a year) and when it is necessary after changes in the plans. See the Guidelines on Business Continuity Management for the different types and frequency of the tests.

(6) Exercising outsourced IT function or services

- As the outsourcing organisation is always fully accountable for the outsourced function or services including IT, it has to require in a contract and under SLAs that the supplier organisation provides evidence of viable continuity plans and results of their exercising.

- This has to be done for suppliers that are other organisations in the Commission or third-parties.

(7) Maintenance and review

- The organization must establish a maintenance programme to ensure that any internal or external change to the organizational 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.

(8) 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 organisation objectives and relevant good practices has to be included in the BCM review.

6. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006

Implementing rules of Commission Decision C(2006) 3602

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

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

7. RELATED STANDARDS AND SUPPORTING GUIDELINES

Guidelines on Business Continuity Management

Standard on Risk Management