Deliverable: D2.2: Desktop Study – Contingency Planning Methodologies and Business Continuity

Version: 1.0

Seventh Framework Programme Theme ICT-SEC-2007-7.0-01

Project Acronym: EURACOM

Project Full Title: EUropean Risk Assessment and Contingency planning Methodologies for interconnected networks

Grant Agreement: 225579

Coordinator: EOS
### Document Control Sheet

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change Status</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>06-11-09</td>
<td>Official release</td>
<td>Dirk Tilsner, David Arouca</td>
</tr>
</tbody>
</table>
## Table of Contents

1 Introduction ........................................................................................................................................... 7
   1.1 Context of EURACOM ....................................................................................................................... 7
   1.2 WP2 Deliverables ............................................................................................................................ 8
   1.3 W 2.2 Objectives ............................................................................................................................ 8
   1.4 Structure of the Document .............................................................................................................. 9
   1.5 Acronyms .................................................................................................................................... 10

2 Analysis Framework ............................................................................................................................ 11
   2.1 Objective of the Analysis ................................................................................................................. 11
   2.2 Approach .................................................................................................................................... 11
   2.3 Concepts and Scope of Contingency Planning and BCM ............................................................... 12
   2.4 Relation to Risk Management ....................................................................................................... 14
   2.5 Selection of Criteria for the Analysis ............................................................................................. 15
      2.5.1 Selection of Resources ............................................................................................................... 15
      2.5.2 Evaluation of Standards and Guidelines ..................................................................................... 16

3 Overview of Standards and Guidelines ............................................................................................. 19
   3.1 International Standards and Guidelines .......................................................................................... 19
      3.1.1 ISO/PAS 22399:2007 ................................................................................................................. 19
      3.1.2 CMMI for Services .................................................................................................................... 20
   3.2 National Standards ........................................................................................................................ 21
      3.2.1 BS 25999-1:2006 / BS 25999-2:2007 .......................................................................................... 21
      3.2.2 BCI Good Practice Guidelines 2008 ....................................................................................... 22
      3.2.3 AS SAA HB 221:2004 .............................................................................................................. 23
3.2.4 ASIS SPC.1-2009 ...........................................................................................................................................25
3.2.5 NFPA 1600:2007 ........................................................................................................................................25
3.2.6 SS 540:2008 ................................................................................................................................................27
3.3 ICT Security Related Standards and Guidelines .........................................................................................29
3.3.1 ISO/IEC 24762:2008 ................................................................................................................................29
3.3.2 NIST Special Publication 800-34 .............................................................................................................31
3.3.3 Other ICT related Standards .....................................................................................................................33
3.4 CIP, Energy and other Utilities ..................................................................................................................34
3.4.1 NERC Reliability Standards and Security Guidelines .............................................................................34
3.5 Examples from Other Domains ..................................................................................................................35
3.5.1 FSA BCM Practice Guide .........................................................................................................................35
3.5.2 BASEL II’s Business Continuity Guidelines ............................................................................................36
3.5.3 FFIEC Business Continuity Planning .........................................................................................................37
3.5.4 Healthcare BCM .......................................................................................................................................38
4 Desktop Study – Comparative Analysis of Selected Standards and Guidelines ..............................................39
4.1 Holistic, general Standards and Guidelines .................................................................................................39
4.1.1 General Categorisation ...............................................................................................................................39
4.1.2 Structural Elements ....................................................................................................................................39
4.2 Sector and Domain-specific Standards and Guidelines ..............................................................................41
4.2.1 General Categorisation ...............................................................................................................................41
4.2.2 Structural Elements ....................................................................................................................................41
5 Conclusions ....................................................................................................................................................43
5.1 Synthesis of the Analysis ..............................................................................................................................43
5.1.1 Matrix of Criteria vs. Standards ..................................................................................................................43
5.1.2 Common Elements and Conceptual Differences ......................................................................................45
Figures

Figure 1: Structure of the EURACOM project.................................................................7
Figure 2: BCM Lifecycle according to BS 25999-1:2006 and other standards..................14
Figure 3: IPOCM flow diagram according to ISO/PAS 22399........................................19
Figure 4: Scopes for BS 25999 Part 1 (BCM lifecycle) and Part 2 (PDCA cycle)...........21
Figure 5: Structure of the guideline components in the BCI Good Practice Guideline....23
Figure 6: BCM process according to HB 221:2004 (adapted)......................................24
Figure 7: BCM Framework of SS 540:2008.................................................................27
Figure 8: ICT DR service provision framework according to ISO/IEC 24762...............29
Figure 9: Disaster Recovery Planning Approach from ISO/IEC 24762:2008....................31
Figure 10: Contingency Planning Process according to NIST 800-34..........................32
Figure 11: Structure of the FSA BCM Practice Guide................................................35

Tables

Table 1: Comparison of Risk Management and BCM according to [BCI, 2008].............15
Table 2: Matrix for Criteria vs. Standards and Guidelines..............................................44
1 Introduction

1.1 Context of EURACOM

The objective of EURACOM is to identify, together with European Critical Energy Infrastructures operators, a common and holistic approach (end-to-end energy supply chain) for risk assessment and risk management solutions. This is to facilitate an increase in the resilience of critical energy services across the whole (‘end-to-end’) energy infrastructure chain.

EURACOM’s activities to define common risk assessment and contingency planning methodologies will build upon the EURAM project results: the EURAM methodology will be specifically developed for the energy sector.

EURACOM has to cover all applicable hazards to the energy sector, including threats from natural causes, human intent, technical failure, human failure, other Critical Infrastructures and other dependencies.

In the development of the EURACOM project, it was apparent that methodological solutions and supporting tools should be developed in close cooperation with European Critical Energy Infrastructure operators. The EURACOM project has been structured accordingly.

In order to develop the methodology and supporting tools, the following structure is applied to the EURACOM project:
1.2 WP2 Deliverables

The role of Work Package 2 (WP2) in EURACOM is the identification of a common and holistic approach for risk assessment and contingency planning. WP2 has three deliverables:

**Deliverable 2.1:** Concerns the analysis of available Risk Assessment approaches to identify good practices from several domains including security industry, national guidance and energy standards.

**Deliverable 2.2:** Which this report addresses, concerns the analysis of Contingency Planning approaches to identify good practices from several domains including security industry, national guidance and energy standards.

**Deliverable 2.3:** Concerns the analysis of the communally accepted links between Risk Assessment and Contingency Planning practices and the creation of Risk Assessment and Contingency Planning approaches which can be combined and are clearly targeted to the energy sector.

1.3 W 2.2 Objectives

The purpose of Work Package 2.2 (WP 2.2) is to document a review of current Contingency Planning Methodologies and Business Continuity Management (BCM) from various sources, encompassing international, national and domain-specific standards and guidelines. Taking into consideration the growing importance of BCM as a holistic approach covering all strategic and operational activities of an organisation, a particular focus was placed on the corresponding standards.

This desktop study is complementary to other activities undertaken within the scope of WP2 – Risk Management Methodologies under the EURACOM project. In this work package, we aim to identify international and European guidelines and good practices for risk assessment and risk management solutions in order to increase the resilience of services across the whole energy infrastructure chain, especially with respect to the different type of malicious (intentional) attacks.

Supported by the EURACOM D2.1 desktop study on risk assessment methods and further analysis of the link between contingency management & BCM and risk assessment methodologies, the report is expected to feed the development of a common EURACOM approach to a risk and contingency management concept and framework that can be applied successfully within the energy sector, with special emphasis being given to interconnections of energy networks, contingency planning interoperability and risk sharing between operators.
1.4 Structure of the Document

The document is structured in five major sections:

- **Section 1:** Introduction (this section)

- **Section 2:** Analysis Framework:
  
  This section describes the objectives of the analysis, work approach and criteria for the selection of sources and their assessment. In addition, the section provides a brief discussion on the scope and definition of Contingency Planning and BCM, their relationship, the relation to risk assessment & management and role in the context of Critical-Infrastructure Protection (CIP).

- **Section 3:** Overview of Standards and Guidelines
  
  The objective of this section is to provide a brief overview of each of the analysed standards and guidelines.

- **Section 4:** Desktop Study – Comparative Analysis of Selected Standards and Guidelines
  
  This section documents the execution of the analysis following the work approach as defined in section 2.

- **Section 5:** Summary and Conclusions
  
  The main elements of the Summary and Conclusions are given by a synthesis of conclusions and key findings of the analysis (see section 5) and by a set of recommendations for the development of a EURACOM planning methodology as planned under this project.
## 1.5 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Planning (or Plan)</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>CM</td>
<td>Crisis Management</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning (or Plan)</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>ICT</td>
<td>Information &amp; Communication Technologies</td>
</tr>
<tr>
<td>IM</td>
<td>Incident Management</td>
</tr>
<tr>
<td>IPOCM</td>
<td>Incident Preparedness and Operational Continuity Management</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>OR</td>
<td>Organisational Resilience</td>
</tr>
<tr>
<td>PDCA</td>
<td>Plan – Do – Check – Act</td>
</tr>
<tr>
<td>PM</td>
<td>Project Management</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>RAM</td>
<td>Risk Assessment Methodology</td>
</tr>
<tr>
<td>RM</td>
<td>Risk Management</td>
</tr>
</tbody>
</table>
2 Analysis Framework

2.1 Objective of the Analysis

The analysis has been structured and undertaken as desktop study following the general objectives as stated in section 1.1:

- To make a qualitative evaluation of existing standards and guidelines for contingency planning and BCM based on a defined set of analysis criteria, and
- To assess the suitability for application in the energy sector, having in mind the goal to develop under this project, a common, holistic EURACOM methodology for risk assessment and contingency planning.

The required information sources have essentially been taken from international and national standardisation organisations and other public information sites on the internet.

The output of this report includes the following key elements:

- A matrix ‘criteria vs. standards/guidelines’ synthesising the results of the analysis,
- A summary of the mandatory elements of a new, holistic approach, with identification of strengths and weaknesses of existing frameworks and methods,
- A compilation of recommendations for the development of a EURACOM approach, taking into account the qualitative conclusions concerning the analysis of existing resources (standards, guidelines), fundamental requirements to be considered for the management of the energy supply chain and so far identified gaps of analysed resources.

2.2 Approach

The analysis follows a straightforward work approach that comprises the following steps:

1. **Selection of resources for analysis**

   The desktop study initiated with the search and the identification of the relevant resources, i.e. standards and guidelines for contingency planning and business continuity. The criteria for this selection are described in section 2.5.1.

2. **Definition of criteria for assessment and comparative analysis**

   After a first review of the available literature, a set of criteria for a more detailed and comparative analysis of the selected resources was defined. As explained in more detail in section 2.5.2, the criteria were based on common elements of the existing methodologies and frameworks. This list was iteratively completed during the course of the analysis (step 3).
3. **Execution of the analysis**

In this step, the selected resources were formally evaluated on the basis of established criteria. In order to ease the reading of the present report, each standard or guideline was described (short summary only) with highlight of the main features, underlying frameworks (e.g. for BCM, flow diagrams etc.), strong points and any limitations. At the same time, the conformance of the standard or guideline with respect to each individual criterion was documented in a spreadsheet.

4. **Conclusion and recommendations**

The final step included a qualitative assessment of the output of the analysis as obtained in the scope of step 3 (execution), i.e. the above mentioned spreadsheet. In order to ensure intuitive interpretation of the content of this table, the matching of each standard or guideline with respect to the criteria was ranked according to standard compliance criteria (full, partial, non-compliant). These results were then compiled into this report.

The final section is a conclusion of the general requirements for a contingency planning approach for the energy sector. These were extracted from the results of other project activities, namely from [EURACOM, 1] that provides an overview of European energy infra-structures and for specific topics of interest.

### 2.3 Concepts and Scope of Contingency Planning and BCM

The concept of contingency planning is easily understood as an approach to prepare for unpredicted, adverse events and circumstances, by defining particular strategies, counter-measures, planning of back-up actions and resources etc. From a general perspective, this can be applied to a project, organisational activity or process or to an entire organisation.

On the other hand, the concept of business continuity is usually seen in the context of an organisation as a whole that aims to ensure critical activities, services etc. at an acceptable level in the case of disruptive events, emergency situations and the like.

Notwithstanding the fact that there is no unique definition for business continuity (management) and contingency planning, (here: in the context of organisational risk management and continuity), available standards and guidelines provide very similar definitions and descriptions as concerns the general organisational scope and objectives, approaches and methodologies as well as key elements and processes. The following citations taken from Wikipedia available on the Internet are given here as examples:

“... *Contingency plans* include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency or state of affairs. They also include a monitoring process and “triggers” for initiating planned actions. They are required to help governments, businesses or individuals to recover from serious incidents in the minimum time with minimum cost and disruption ... “

“... **Business continuity** is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business Continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability ...” ([http://en.wikipedia.org/wiki/Business_continuity](http://en.wikipedia.org/wiki/Business_continuity)).

It is important to be aware that the scope of business continuity is not limited to the activation of a continuity and recovery plan once a disaster event or equivalent has occurred, but should be seen as a management process being implemented and supporting daily operations. As a matter of fact, Business Continuity Management (BCM) standards and practices have evolved significantly over recent years, moving the emphasis “… from the more traditional mainframe disaster recovery planning in the domain of the IT department, through crisis management planning and business continuity planning to the more expansive concept of BCM. Progressively more organisations now regard BCM not as a costly planning process, but as a key value added improvement process firmly integrated within risk management …” [Standards Australia International / Standards New Zealand, 2004].

In this analysis we maintain the emphasis on business continuity and contingency planning as a holistic management process (i.e. BCM) integrated within the risk management family of processes. As a matter of fact, most available BCM standards and guidelines rely on very similar frameworks and process models, encompassing the following key elements:

- The analysis of the organisational context (e.g. organisational and (strategic, operational) business objectives, relationships with other organisations and responsibilities) and the identification of critical activities and resources (business impact analysis, continuity requirements, threat assessment, choices for risk and continuity management),

- The definition of a BCM policy and strategy (e.g. BCM scope within the organisation, key processes and requirements covered, relevant regulations or policies, general strategy and options for critical activities and resources (people, infrastructure, supplies etc.), principles, guidelines and minimum standards),

- The development and implementation of BCM (planning for the management of incidents, emergencies, continuity and recovery),

- Exercising, maintaining and review (programmes for exercising the BCM process as a whole or for particular elements and plans, training, arrangements for review, maintenance and continuous improvement),

- Programme management (arrangements for the implementation of the BCM programme, e.g. organisational structure and responsibilities, documentation, management activities),

- Embedding BCM in the organisation’s culture (strategies and measures ensuring that the efficient implementation of BCM across the whole organisation and according to the BCM strategy set out, awareness, training and general preparation).
The listed elements incorporate a process that is often referred to as BCM Lifecycle as shown in the following figure as taken from [BSI, 2006]. The reader should bear in mind though that the analysis underlying this report did not aim to establish any preference for a particular BCM model or framework, and that the described key elements may be grouped and associated in a different manner:

![BCM Lifecycle diagram](image)

**Figure 2: BCM Lifecycle according to BS 25999-1:2006 and other standards.**

### 2.4 Relation to Risk Management

It is straightforward to see that BCM and contingency planning are an integral part of the risk management collection of processes. The majority of standards and guidelines incorporate or at least refer to risk management activities such as threat/risk and vulnerability assessment and risk treatment (mitigation, transfer etc.).

It is true though that a considerable number of standards and guidelines fail to describe the relation to risk management in a clear way. Whilst some standards have in fact to be seen in the context of co-existing (overarching or complementary) standards for risk management (issued by the same standardisation organisation; the BCM standard is part of a wider set of organisational management standards), others simply include risk assessment and other particular activities without establishing a clear link to a general risk management process out of the scope of BCM.

An organisation should always regard risk management as one key process and integrated part of daily operations management, irrespective of the existence of particular plans for business continuity, disaster recovery etc. From this point of view, the existence of risk management practices and procedures should be seen as an input for BCM planning and implementation. The extent to which risk management and BCM appear as integrated processes also depends on the very scope of BCM according to the organisation’s BCM strategy, focussed on the most critical activities and resources and associated continuity objectives. This
conceptual difference in scope is illustrated in the following table taken from the BCI Good Practices Guidelines 2008:

<table>
<thead>
<tr>
<th></th>
<th>Risk Management</th>
<th>BCM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key method</strong></td>
<td>Risk analysis</td>
<td>Business impact analysis</td>
</tr>
<tr>
<td><strong>Key parameters</strong></td>
<td>Impact and probability</td>
<td>Impact and time</td>
</tr>
<tr>
<td><strong>Type of incident</strong></td>
<td>All types of events, though usually</td>
<td>Events causing significant business</td>
</tr>
<tr>
<td></td>
<td>segmented</td>
<td>disruptions</td>
</tr>
<tr>
<td><strong>Size of event</strong></td>
<td>All sizes (costs) of events, though</td>
<td>Strategy is planned to cope with</td>
</tr>
<tr>
<td></td>
<td>usually segmented</td>
<td>survival-threatening incidents but can</td>
</tr>
<tr>
<td></td>
<td></td>
<td>manage any size of incident</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Focus primarily on management of risks</td>
<td>Focus mainly on incident management mostly</td>
</tr>
<tr>
<td></td>
<td>to core-business objectives</td>
<td>outside the core competences of the business</td>
</tr>
<tr>
<td><strong>Intensity</strong></td>
<td>All from gradual to sudden</td>
<td>Sudden or rapid events (though response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>may also be appropriate if a creeping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>incident becomes severe</td>
</tr>
</tbody>
</table>

Table 1: Comparison of Risk Management and BCM according to [BCI, 2008].

2.5 Selection of Criteria for the Analysis

2.5.1 Selection of Resources

The identification of potential resources for the analysis took into consideration basic and fundamental criteria such as:

- **Purpose:**
  - Contingency Planning and Business Continuity
  - standard vs. (operational, practice) guidelines

- **Scope:**
  - holistic, general applicability vs. sector-specific (energy, utilities, Information and Communication Technologies (ICT), other)
  - international vs. national (European vs. outside EU)

In the scope of the search for relevant resources it was identified that good operational practices in particular from European operators were not publicly available, but that they could however be obtained through a consultation process at later stages in the project (WP3 - End-to-end energy chain Community & Forum, WP4 - Preparation work, scenarios & case analysis for common issues, risk factors, threats of interconnected energy networks workshops). It was therefore decided to exclude a questionnaire or equivalent approach to collect this information, but to focus on available international and national standards in the areas of contingency planning and business continuity.
It was also found that the majority of standards were either international (i.e. endorsed by international standardisation organisations such as ISO) or national within countries such as the UK, USA & Australia. Many of these standards are applied and/or used as reference in a larger number of countries around the world, mainly due to the international reputation of the corresponding organisations (e.g. BSI British Standards, ASIS International).

Energy sector-specific resources were identified primarily from the US (see references from NERC, NIST and DoE) and were considered in the analysis. It should be emphasised that the analysis formally addressed only the structural elements (main steps and their objectives, underlying planning documentation etc.) of these standards and guidance documents, leaving out any regulatory, legislative or specific organisational aspects that could lead to conclusions with limited applicability for the European market. In the case of the NERC Security Guidelines, these were found to be insufficiently structured and detailed for the purpose of this study, but were kept for general discussion and for the sake of completeness.

Due to the limited availability of energy sector specific standards and methodologies, the scope of the analysis was broadened to include and consider other domains and sectors. There are a considerably large number of ICT related standards and guidelines that are available, and a few representative examples were selected for inclusion within the analysis. It should also be mentioned that these references were also analysed taking into consideration the identification of common, structural elements, leaving out any ICT-specific elements. The same principle was applied in the case of other sector-specific (e.g. finance) resources.

2.5.2 Evaluation of Standards and Guidelines

The criteria for the evaluation of the identified resources were selected in a manner that safeguards the principles of comparability (e.g. general standards vs. domain-specific standards), placing the focus on key features as well as common and unique structural elements (steps and activities, objectives for each of these, documentation, recommended methodology and/or template etc.). Hence, the set of criteria for analysis was defined on the basis of a first screening of resources:

General categorisation:

- **Standard** (auditable, certified) or de-facto standard
- **Guideline**, i.e. guidance for operational use handbook, good practices etc. (note that a standard may have associated a guidance document or similar)
- **Holistic approach** (i.e. general, not specific for a certain domain) vs. domain (e.g. ICT disaster recovery) or sector (e.g. financial, energy) specific – reference which sector
- **Energy sector** specific, i.e. either by origin or by documented application of the standard, guideline etc. (note that a standard may be holistic, but has been applied to a specific sector)
- **International** vs. national (identify country)
- **Framework**, i.e. formal framework exists (identify which, e.g. BCM, reference to PDCA etc.)
Structural elements:

The majority of the following elements have been extracted from BCM frameworks and considering the common view as discussed above (section 2.3). The analysis should consider that the elements contained by non-BCM standards and guidelines may still have a direct correspondence with these elements.

• **Programme management**
  - Assigning **Responsibilities**
  - Recommended or mandatory **Documentation** plan (for some or all phases)
  - **Strategy / Policy** definition (in the scope of this analysis considered equivalent)
  - **Regulation**, i.e. regulatory and legal constraints and related requirements

• **Organisational analysis**
  - **BIA** (Business Impact Analysis)
  - Identification of **Critical activities**
  - **Continuity requirements**
  - **Risk and vulnerability analysis**
  - Procedures for the evaluation and selection of measures, **Choices**

• **Components**
  - **People**
  - **Infrastructure** (premises, equipment etc.)
  - **Information**
  - **External dependencies** (supplies, stakeholders etc.)
  - **Environment**
  - **Continuity** of service operations
  - **Other**

• **Development and implementation of response**
  - **Incident prevention** (risk mitigation, prevention strategies and plans)
  - **Emergency preparedness** (scope and context, planning of resources)
  - **Business continuity** (continuity planning)
  - **Response management** (incident or emergency planning)
  - **Recovery** and restoration of normal activities
  - **Other** implementation issues: resources requirements, financial administration, operational control
D2.2 Contingency Planning and Business Continuity Methodologies

- **Process Management**
  - Performance assessments (of implemented BCM program or equivalent)
  - Different methods for Exercising
  - Maintenance and review cycle and procedures
  - Continuous improvement

- **Organisational preparation and culture**
  - Awareness, Communication
  - Training

For each group, the existence of recommendations for particular methodologies and/or templates shall be indicated.
3 Overview of Standards and Guidelines

3.1 International Standards and Guidelines

3.1.1 ISO/PAS 22399:2007

As suggested by its title “Societal security – Guideline for incident preparedness and operational continuity management” (abbreviated as IPOCM), this ISO standard published in 2007 shall be understood as a guideline for establishing the process, principles and terminology for IPOCM applied to any kind of public or private, business or non-profit organisation. Understanding IPOCM as a holistic management process, the guideline addresses all fundamental phases from preparedness/prevention, emergency response and business continuity to recovery, except for specific emergency response activities such as disaster relief and social infrastructure recovery:

Figure 3: IPOCM flow diagram according to ISO/PAS 22399.
The standard describes for each of the phases presented in the above figure the general principles, objectives, criteria and controls that are based on good practices, does however not propose particular methodologies to be adopted for particular activities. A certain exception is given by a number of informative annexes that include a generalised impact analysis procedure as well as general structures for emergency response management and continuity management programs.

**Strengths:**

This standard is compliant with virtually all of the established criteria and includes informative annexes for additional guidance. Incident prevention and mitigation is particularly addressed.

**Potential limitations:**

In comparison to other standards and guidelines, some critical elements such as risk assessment and vulnerability analysis could be covered with more descriptive detail. The application of the standard may be hampered by the fact that the textual descriptions are not complemented by listed specifications that could serve as check-lists or equivalent.

The reader should be reminded that the standard ISO Technical Committee 223 for Societal Security is also working on ISO/TC 22301 - Preparedness and continuity management systems – Requirements and other relevant areas such as Inter/Intra organisational warning procedures (ISO/NP 22322), Societal security - Principles for command and control, coordination and cooperation in resolving incidents (ISO/CD 22320) and others.

### 3.1.2 CMMI for Services

CMMI stands for Capability Maturity Model Integration and is provided by the Software Engineering Institute (SEI) as collections of good practices for process improvement in the development of products and services covering the entire product lifecycle from conceptualisation through maintenance and disposal. In this context, the CMMI model for services, published only recently in 2009, was developed addressing the particular needs of the service industry.

The CMMI model does not contain a full BCM framework, but describes the particular CMMI methodology for risk management and continuity of services in two particular sections, further establishing the relationship between both.

Risk management covers key elements such as the definition of a risk model (categories, parameters) and of a risk management strategy, risk identification, analysis, evaluation and prioritisation as well as the development and implementation of a risk mitigation plan. Service Continuity (SCON) uses the outputs of risk management and contains the most important steps for continuity management, i.e. the identification of essential functions and resources, the establishment of a service continuity plan and its verification, validation and maintenance as well as training plan preparation and execution.
Strengths:

The guideline (good practices collection) encompasses all fundamental processes of service delivery and the sections on risk assessment and service continuity are only two of these processes. From this perspective, the guideline is certainly useful for service providers that wish to implement a CMMI model for the whole organisation. For this purpose, the less complex structure for service continuity is justified.

Potential limitations:

CMMI for services is not recommended as framework for service continuity in more complex organisations, or even in the domain of critical infra-structures. The level of detail is clearly insufficient; important aspects such as incident prevention, emergency preparedness, the definition of continuity requirements and recovery are only weakly addressed or not at all mentioned.

3.2 National Standards

3.2.1 BS 25999-1:2006 / BS 25999-2:2007


A particular section is dedicated to an overview of BCM in accordance with the general BCM lifecycle, whereas the following sections presents a more detailed description of each BCM lifecycle element (major phase).

![Image of BCM lifecycle and PDCA cycle](image)

Figure 4: Scopes for BS 25999 Part 1 (BCM lifecycle) and Part 2 (PDCA cycle).
The standard takes a holistic approach such as all general BCM standards. It is interesting to note though that organisational resources such as people, premises, technology, information, supplies and stakeholders are specifically addressed as for example opposed to ISO/PAS 22399. Still, the level of detail for these sections remains high and is for example for the area of ‘technology’ not comparable with other ICT-specific BCM standards and guidelines. Part 1 further provides general structures and key elements for the various management plans (incident management, business continuity, recovery).

Part 2 of the standard specifies the requirements with regard to the principles and practices contained with Part 1, with focus on those requirements that can be objectively audited. In line with other management standards, Part 2 applies the PDCA (Plan – Do – Check – Act) cycle that aims to ensure that business continuity is effectively managed and improved. The different scopes of the two parts of the standard are illustrated in the figure above (taken from the standard).

In Part 2, requirements are specified for each of the BCM lifecycle phases and with more level of detail (but also repetitions) as in Part 1. This includes for example specific requirements for business impact analysis (e.g. maximum time periods for resumption of activities after disruption), elements of BC and IPM plans and monitoring and review activities, not proposing though the application of particular methodologies and tools.

**Strengths:**

BS 25999 is one of the most widely-known BCM standards up to date. It is very complete and has a clear focus on business continuity. Specifications are provided in a structured way that supports well adoption and implementation.

**Potential limitations:**

Incident prevention and business recovery are not addressed by the standard, as this concentrates on incident response and management and business continuity.

### 3.2.2 BCI Good Practice Guidelines 2008

This guide has been published in its first version by the Business Continuity Institute (BCI) in 2002 and has driven the standard development by the British Standards Institution’s (BSI). Being closely related to BS 25999, this guideline may be viewed as the most exhaustive description of the BCM framework underlying the British (and a series of other) standards. For the given reason, the guideline has virtually the same scope as BS 25999.

An interesting aspect though is the structure of the description of all guideline components, turning this document into a valuable, complementary resource for organisation or individuals who wish to apply and implement the BSI standard.
3.2.3 AS SAA HB 221:2004

This is the Australian Guideline for Business Continuity Management as developed by Standards Australia / Standards New Zealand and it is accompanied by AS SAA HB292:2006 “A Practitioners Guide To Business Continuity Management” and AS SAA HB293:2006 “Executive Guide To Business Continuity Management”.

Presented as “Handbook” (not being considered as true standard), this guide is divided into two major sections:

- an overview of BCM including a description of the relationships with regard to risk management, corporate governance, interdependencies etc.,

- a BCM manual that summarises all information on the basis of a simple table structure for each phase – step / desired outcome / activities; the manual further offers some non-mandatory templates for business impact analysis, minimum resource requirements, continuity plan, communications strategy etc.

The guideline follows a standard BCM process, with slight differences though with respect to the BSI standard for example, considering the nine steps in the BCM process as shown in the figure below. For example, risk and vulnerability assessments are introduced as a distinct step before Business Impact Analysis.

**Strengths:**

The handbook’s value resides in its simple, straightforward structure, capturing virtually all essential elements contained by more detailed specifications (standards) and guidelines (with the limitations identified below). It therefore seems to be well suited for organisations with little BCM experience and/or complexity. This idea is further supported by the set of templates in the BCM Workbook; these may at least

---

<table>
<thead>
<tr>
<th>Guideline component</th>
<th>Questions answered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td></td>
</tr>
<tr>
<td>Precursors</td>
<td>What needs to be done before this?</td>
</tr>
<tr>
<td>Purpose</td>
<td>Why do we need to do it?</td>
</tr>
<tr>
<td></td>
<td>What will it achieve?</td>
</tr>
<tr>
<td>Concepts and Assumptions</td>
<td>What do we need to understand?</td>
</tr>
<tr>
<td></td>
<td>What assumptions are we making?</td>
</tr>
<tr>
<td>Process</td>
<td>What do we need to do?</td>
</tr>
<tr>
<td>Methods and Techniques</td>
<td>What are the tools we need to do it?</td>
</tr>
<tr>
<td>Outcomes and Deliverables</td>
<td>What should it produce?</td>
</tr>
<tr>
<td>Review</td>
<td>When should it be done?</td>
</tr>
</tbody>
</table>

**Figure 5: Structure of the guideline components in the BCI Good Practice Guideline.**
be seen as a starting point for the structuring of a BCM process implementation. Interestingly, the identification of external interdependencies is specifically addressed.

**Potential limitations:**

The simplicity comes at the cost of (the handbook) not providing more detailed provisions (similar to specifications that could be checked for implementation one-by-one) for all steps. For example, it is not always clear how ‘Activities’ and ‘Desired Outcomes’ are effectively related to each other, whereas some important topics are described in a way that can be regarded as superficial (e.g. Step 4: Response Strategies just mentions the need to determine criteria for emergency, continuity and recovery response, but does not go into any relevant detail).

Another limitation is given by the fact that important elements as contained in other BCM frameworks are not or only weakly addressed. For example, HB 221:2004 is the only guideline that does not distinguish between exercising (e.g. running incident management scenarios) and training. Similar considerations can be made with regard to incident prevention, BCM choices and continuous improvement.

![BCM process according to HB 221:2004 (adapted).](image)
3.2.4 ASIS SPC.1-2009

This is the recent ASIS standard for organisational resilience. As a matter of fact, the scope is very similar to the ISO/PAS 22399, including the flow diagram for the Organisational Resilience (OR) Management System (term used instead of IPOCM, see Figure 2). The standard adopts the PDCA model which is reflected by the structure of the OR process (Plan – planning, Do – implementation and operation, Check – checking / evaluation, Act – management review / review and maintain the management system).

The two most important sections of the standard contain:

- the requirements for an OR management system,
- a guidance summary of the use of the standard.

The requirements section specifies in a rather concise manner (on only 14 pages) what exactly an organisation shall do in order to apply the standard. The guidance section is far more descriptive and explains why and how the requirements specifications can be met.

The standard also contains a guidance section as well as a table with correspondence to other ISO standards (ISO 9001:2000, ISO 14001:2004, ISO 27001:2005), but strangely not with other BCM frameworks and standards.

**Strengths:**

As mentioned, the standard has essentially the same scope as ISO/PAS 22399. In comparison to the latter, requirements are formulated in a specification style (listed set of requirements per topic) which supports better implementation. On the other hand, the additional guidance section provides additional clarifications for implementation. Formally, all criteria of the analysis are met.

**Potential limitations:**

Similar to ISO/PAS 22399, a strong focus is placed on incident prevention, preparedness and management, including crisis management. Business continuity is embedded in this model, however with less emphasis than in typical BCM standards. Documentation is addressed, however, no particular structure for a documentation plan or templates for typical documents are presented.

3.2.5 NFPA 1600:2007

This American Standard on Disaster/Emergency Management and Business Continuity Programs published by the National Fire Protection Association (NFPA) in 2007 for “Disaster/Emergency Management and Business Continuity Programs” has evolved from former guides for disaster management. As concerns the scope of NFPA 1600, and as pointed out in the standard, the program elements are applicable to prevention, mitigation, preparedness, response, and recovery.

The recommended process relies on a program structure that is summarised as follows:
– Program Management
  o administration, coordinator, advisory committee, program evaluation

– Program Elements
  o general
  o laws and authorities
  o risk assessment
  o incident prevention
  o mitigation
  o resource management and logistics
  o mutual aid / assistance
  o planning (includes planning process, common plan elements, plans)
  o incident management
  o communications and warning
  o operational procedures
  o facilities
  o training
  o exercises, evaluations and corrective actions
  o crisis communication and public information
  o finance and administration

The standard includes explanatory material providing additional guidance; however the descriptive detail is not comparable with other guidance documents and sections as attached to other standards.

It is interesting to analyse because it does not closely follow what could be called a standard BCM approach and framework as other standards do. It should be mentioned that the document provides a kind of map with regard to BCI (Business Continuity Institute) & DRII (Disaster Recovery Institute International) Professional Practices, showing how NFPA 1600 links with other (typical) business continuity frameworks.

**Strengths:**

This standard specifies all requirements (programme elements) in a very clear, concise and synthetic way. This can be seen as advantage from the perspective of standard implementation and formal verification of compliance. The explanatory material places particular emphasis on risk assessment (hazard identification, assessment techniques).
Potential limitations:

The indicated strength has the downside that more detailed guidance for implementation is not provided, therefore the standard will be difficult to adopt by inexperienced organisations. The non-typical program structure should not be seen in itself as a disadvantage, however NFPA 1600 does not appear to capture all the typical elements of the other typical BCM standards. In particular, the requirements specifications and explanatory notes on business continuity (requirements definition, elements of the continuity plan, choices) appear to be quite superficial in comparison to other standards. Similar considerations can be made with respect to exercising and maintenance and review (nonetheless a Corrective Action Program is described with some more detail).

A decisive disadvantage stems from the fact that the standard is explicitly aimed at an American audience, i.e. it contains (as opposed to other national standards that manage to maintain a generic structure and description) a series of terms and references to organisational and regulatory aspects (e.g. for emergency management) that would be difficult to cross referenced to other national or organisational specificities.

3.2.6 SS 540:2008

This is the Singapore Standard (SS) for BCM published by SPRING Singapore, following an earlier specification TR (Technical Reference) 19:2005. According to the standard, it “... adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving and organisation’s preparedness, response and continuity management system.” The way the BCM framework is presented is slightly different from the conceptual frameworks found in other standards:

![BCM Framework of SS 540:2008.](image)

As shown in the figure above, the BCM framework consists of a matrix containing the essential BCM components (columns) and six BCM areas (lines). As concerns the latter, the sequence of these areas may
propose the notion of a process and corresponding flow of major activities. The standard claims to adopt the PDCA methodology, covering the whole cycle from planning (Plan), implementation and operation (Do), monitoring and checking (Check) and maintenance and continual improvement (Act). However the sequence of BCM areas does not convincingly prove the complete adoption of the PDCA approach as a cyclic process. It should be added that the sample table of contents of a BCM Manual provided in an annex is also structured according to the identified main BCM areas.

On the other hand, the specifications for each BCM area address are based on a structure embedding the definition of the scope and all BCM components shown in the figure above.

**Strengths:**

This standard presents a slightly simplified macro-structure of the BCM process, ensuring though that all selected criteria for the analysis are covered. The matrix-based approach ensures that all essential BCM components are addressed and described with a comparable level of detail for all BCM areas. This kind of homogeneity is in fact not always present in all analysed standards and guidelines.

Risk analysis and review is identified and dealt with as one major BCM area as opposed to other standards that presume that business continuity management relies on an existing risk management process, hence addressing the whole area of risk analysis and management only marginally in the BCM standard or guidance document.

**Potential limitations:**

As discussed above, the chosen approach does not well reflect the PDCA as a cyclic process.

The standard does not propose a minimum set of documents supporting standard implementation and the presentation of the sample table of contents for a general BCM Manual in the annex suggests a level of simplification (that only this single document is sufficient) that is not in line with the documentary baseline as proposed by other standards and guidelines. It should be noted here that the list of BCM areas includes the area “Business continuity plan” and this section and proposed BC plan encompass all activities such as incident and emergency preparedness, response, recovery and resumption of critical business functions and general restoration of all business activities.

The standard would gain value if accompanied by a guidance section. This could include additional clarification on the documentation plan required for standard implementation.
3.3 ICT Security Related Standards and Guidelines

3.3.1 ISO/IEC 24762:2008

This ISO standard provides guidance on the provision of information and communications technology disaster recovery services as part of business continuity management. Due to this particular focus, the standard is not directly comparable to other BCM standard and guidelines. The analysis was nevertheless found to be worthwhile as it demonstrates how ICT disaster recovery fits into the far more comprehensive frameworks for business continuity management, showing where the underlying methodologies are equivalent (same type of process steps, activities) and where a pure ICT disaster recovery approach fails to address other important aspects of an integrated and holistic BCM approach.

As regards the scope of the standard, it should be mentioned that ISO/IEC 24762 bases on an ICT DR Service provision framework as depicted in the following figure. It is straightforward to see that the central elements of analysis (policies, performance measurement, processes and people) correspond to typical BCM components in other standards (see SS 540:2008):

![Figure 8: ICT DR service provision framework according to ISO/IEC 24762.](image)

For the sake of clarity, it should be reminded that this standard is part of a wider set of ISO standards that are strongly related, namely concerning the so called ISO27K standard family:

This includes for example risk assessment and treatment, security incident management, business continuity management and related topics.

- ISO/IEC 27003: Information technology -- Security techniques -- Information security management system implementation guidance (final draft, for 2009 or 2010)
  - This standard also covers risk assessment and planning risk treatment.


The most relevant standard for our analysis would be ISO/IEC 27031, indeed. This specification is currently in the drafting stage and hence, not yet publicly available. As the title suggests, it will provide a framework for ICT readiness for business continuity, covering incident, business continuity, disaster recovery, and emergency response and related management processes. It is further anticipated that the standard will incorporate a PDCA cycle.

The ISO/IEC 24762 requirements are specified for implementing, operating, monitoring and maintaining ICT disaster recovery services, distinguishing between in-house and outsourced service provision. This need for this differentiation may not be understood immediately. For in-house service providers, the standard establishes the relation between ICT DR and the organisation’s business continuity planning (as a matter of fact, disaster recovery is not presented as one distinct part of the overall BCM process). On the other hand, for outsourced service providers the standard recommends an overall disaster recovery planning approach. As shown in the figure below, this recommended approach contains typical steps of a common BCM process, such as risk assessment, impact analysis and the definition of recovery requirements and priorities.

The analysis confirms the existence of fundamental differences in the scope of the standard. This conclusion carries for example the message that a sole ICT disaster recovery approach is by far not sufficient to fulfil general business continuity needs for an organisation, even if the majority of critical business functions depends heavily on the ICT infrastructure composed of systems, data, applications and services etc.

**Strengths:**

This standard is not holistic and concentrates on ICT disaster recovery. It is therefore far more detailed and specific for a number of specific ICT security aspects. This implies that ISO/IEC 24762 and equivalent standards and guidelines can be used complementarily to BCM standards for organisations whose critical activities depend to a large extent on ICT infrastructures.

**Potential limitations:**

The standard does not manage nor aim to substitute other BCM standards and guidelines. Even though this is understood easily, it is not clear why the recommended Disaster Recovery Planning Approach is not described in more detail, i.e. as process and for all fundamental components. For example, business impact analysis and risk assessment as well as the definition of recovery (continuity) requirements are not dealt
with (just mentioned) and no particular documentation plan (for the implementation of a DR planning approach) is recommended.

Figure 9: Disaster Recovery Planning Approach from ISO/IEC 24762:2008.

3.3.2 **NIST Special Publication 800-34**

This American guide published by NIST (National Institute of Standard and Technology) is entitled *Contingency Planning Guide for Information Technology (IT) Systems*. It is interesting to note that the underlying IT contingency planning process is seen in the context of a “… *overall Continuity of Operations Plan and Business Continuity Plan process.*” As concerns the scope, the guide also clarifies that “… *contingency planning refers to interim measures to recover IT services following an emergency or system disruption.*”

The analysis of this standard is interesting because the underlying methodology clearly contains some important elements of a common BCM framework. In other words, NIST SP 800-34 is much closer to the holistic BCM standards and guidelines than ISO/IEC 24762 or other ‘typical’ ICT recovery standards. The presented contingency planning process encompasses many essential elements of a typical BCM process and consists of the following steps:
The document provides guidelines for each of the phases of the process, with clear focus on ICT aspects. The annexes further provide a sample IT contingency plan format as well as a sample and template for business impact analysis.

The guide also establishes the relationship with other types of contingency related plans (e.g. for cyber incident response, disaster recovery etc.) and should be regarded as complementary with NIST 800-30, the guide for risk management for IT systems.

**Strengths:**

This guide provides a comprehensive view on contingency planning for ICT, i.e. as planning process. As mentioned above, this underlying process has a similar structure of analysed BCM frameworks

**Potential limitations:**

In accordance with the general purpose and scope of the guide, not all BCM equivalent elements are addressed with the same level of detail. As a matter of fact, the most important implementation aspects are related to preventive controls (preventive measures that deter, detect, and/or reduce outage impacts to a system) and recovery strategies and their implementation (procedures, activities).

**DOE CIO Guidance CS-7**

This US guidance document (Contingency Planning Guidance) concerns the implementation of NIST 800-34 and was elaborated under the Cyber Security Program of the US Department of Energy. The general scope is therefore equivalent with NIST 800-34, however, additional guidance is provided only for a few elements and activities of NIST 800-34 (recovery in general). As a matter of fact, DOE CIO Guidance CS-7 is far more synthetic as NIT 800-34 itself. Notwithstanding these facts, the document has formally been included in the analysis and is treated as independent reference.
3.3.3 Other ICT related Standards

In the area of ICT, a larger number of other standards and guidelines exist and could be used for further analysis. The interested user may be referred to the following three examples:

ANSI/ISA-99.02.01 Outlines Industrial Cyber Security Management Systems, more information at http://www.isa.org/

CCTA’s IT Infrastructure Library (ITIL), version 4.2, more information at http://www.itil.co.uk/

BSI Standard 100-1 Information Security Management Systems (ISMS), BSI Standard 100-2 IT-Grundschutz Methodology, more information at http://www.bsi.bund.de/grundschutz

A preliminary analysis of these references confirmed the similar scope, strengths and shortcomings of ICT-focused approaches and methodologies. In order not to further expand the formal analysis of relevant standards and guidelines, the sources discussed in the above sections (3.3.1 and 3.3.2) were considered as sufficient and representative.
3.4 CIP, Energy and other Utilities

3.4.1 NERC Reliability Standards and Security Guidelines

NERC (North American Electric Reliability Corporation) is an independent, non-profit organisation promoted by the electric utility industry whose mission is to ensure the reliability of the bulk power system in North America. In this role, NERC develops standards for Critical Infrastructure Protection (CIP) and other security guidelines and reliability standards for energy infrastructure operators\(^1\). The most relevant standards and guidelines for EURACOM (see [NERC, 2009-1, NERC, 2009-2]) are the following:

- NERC CIP standards, namely CIP-002 through CIP-009; these provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System, concerning for example the physical security of critical cyber assets, security system management, incident response planning and reporting and recovery plans;

- Standards EOP-00x-x; these provide guidance for Emergency Operations Planning (EOP), addressing for example the set up of EOP plans, capacity and energy emergencies (alerting, monitoring etc.), load shedding plans, system restoration planning and coordination etc.;

- Standards IRO-00x-x; these contain the arrangements for Interconnection Reliability Operations and Coordination (IRO), addressing issues such as responsibilities and authorities, facilities, operations planning, transmission loading relief etc.

- Security Guidelines for the Electric Sector; these guidelines were first released in 2002 and describe general approaches, considerations, practices and planning philosophies for electric infrastructure protection, for example for vulnerability and risk assessment, threat response, physical security, cyber security, communication and also continuity of business processes.

Notwithstanding the fact that all of the mentioned standards and security guidelines concern relevant and specific security issues, most of which can easily be mapped to the key elements of typical BCM processes (see section 2.3), they do not compose a general framework or process model comparable with the BCM and contingency planning standards and guidelines discussed so far, and the specifications do not have a comparable level of detail either. For this reason, NERC standards and security guidelines were excluded from the formal analysis.

Nevertheless, the set of standards and guidelines constitute a valuable reference that provides insight into the operational aspects for security management as currently applied (in conformance with the applicable standards) by North American electric infrastructure operators. This includes arrangements and specifications for security in the context of the management of interconnection, power load balancing and other aspects with relevance for EURACOM.

\(^1\) Detailed information can be found at [www.nerc.com](http://www.nerc.com)
3.5 Examples from Other Domains

3.5.1 FSA BCM Practice Guide

A few examples for BCM standardisation efforts and good practices compilation can be found for the financial sector (see also further sections below). The FSA BCM Practice Guide has been selected for analysis not only as the most exhaustive example found for this sector; it also provides a snapshot of the current status and level of application of BCM practices (even if limited to the UK).

The guide is from 2006 and has been issued by the UK FSA – Financial Services Authority. It aims to synthesise best practices obtained from more than 60 firms (answering more than 1,000 questions on their business continuity arrangements) in the scope of the Resilience Benchmarking Project carried out in 2005 by the Tripartite Authorities (FSA, Bank of England and HM Treasury) designed to assess the resilience and recovery capability of the UK financial services sector in the event of major operational disruptions such as a terrorist attack or natural disaster.

The document does not provide the view of a BCM process, but gathers observed practices in the thematic areas listed below. As a matter of fact, the guide stresses the fact that it does not claim to be exhaustive in terms of explaining all elements of a typical business continuity programme and practices relevant for a financial firm.

![Figure 11: Structure of the FSA BCM Practice Guide.](image-url)
For all listed themes, the guideline selects key elements and continuity practices and lists observed standard practices as well as observed leading practices as taken from the above mentioned benchmarking project.

**Strengths:**

The guide focuses on the essential business continuity elements that an organisation operating in the financial sector should consider as relevant. The synthesis of best practices is clear and synthetic.

**Potential limitations:**

Even for financial firms, the document cannot be used as guidance for full implementation of a BCM programme and system (neither is this the purpose of the guide). In comparison to BCM standards and other guidelines, it leaves out or addressed weakly a number of generally important BCM aspects such as business impact analysis and the identification of critical activities (focus is mainly on critical assets and IT infrastructures rather than business processes and activities, except for transactions), criteria for the definition of continuity requirements (recovery time objectives), continuity management alternatives (choices), incident prevention and preparedness (as the focus is mostly on recovery of critical assets, especially IT resources and infrastructures, communications etc.). Best practices on process management are sparse.

### 3.5.2 **BASEL II’s Business Continuity Guidelines**

The so called Basel II Accord, ratified in June 2004 by the 13-member nations of the Basel Committee for Bank Supervision, is a broad, sweeping mandate for capital and risk management reform for the global banking system. The accord provides guidance to banks in three areas (called pillars): (1) the calculation of minimum regulatory capital requirements for credit and operational risks, (2) the supervisory review process, and (3) market disclosure.

The Basel Committee issued Sound Practices for the Management and Supervision of Operational Risk to further the dialogue with the financial services industry regarding the development of sound practices in a number of specific areas of operational risk, such as business continuity. The sound practices documentation includes 10 operational risk management principles and can be viewed as a how to for the Pillar 2 portion of Basel II, even though it is regarded as independent from the formal accord\(^2\). The Sound Practices contain a set of principles grouped under the following topics:

- Developing an Appropriate Risk Management Environment
- Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control
- Role of Supervisors
- Role of Disclosure

\(^2\) This information has been taken from [http://www.continuityinsights.com/Magazine/Issue_Archives/2005/01-02/basell.html](http://www.continuityinsights.com/Magazine/Issue_Archives/2005/01-02/basell.html) and further synthesised.
The second area (Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control) encompasses the Principle 7: \textit{Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.} For this principle, a number of recommendations are given, synthesised as follows:

- The banks should establish disaster recovery and business continuity plans, based on identified vulnerabilities and plausible scenarios,
- Banks should identify critical business processes, including those depending on external vendors or other third parties,
- Banks should periodically review their disaster recovery and business continuity plans maintaining these consistent with the bank’s current operations and business strategies; plans should be tested periodically.

Even taking into consideration that these elements are complemented by other Principles and associated recommendations, it is evident that the Sound Practices do establish a BCM framework or process model. These kinds of guidelines were therefore excluded from the formal analysis.

\subsection*{3.5.3 FFIEC Business Continuity Planning}

The Federal Financial Institutions Examination Council (FFIEC) is an US American interagency body responsible for establishing the standards to which financial institutions are held. The FFIEC has made several publications concerning business continuity, including individual booklets specific to various risk management disciplines.

In 2003, the FFIEC updated Chapter 10, Corporate Contingency Planning, based on the 1996 FFIEC Information Systems Examination Handbook, to reflect new technologies, business practices and the threat of terrorism impacting the availability of critical banking processes and technologies. The 2003 version, or “Gold Standard” as many business continuity professionals refer to it, emphasised the importance of business process response and recovery, as opposed to a program focused almost exclusively on technology availability. This marked a key evolutionary point in financial services business continuity planning.

The newly-released 2008 FFIEC Business Continuity Planning booklet\textsuperscript{3} [FFIEC, 2008] continues to incorporate new business continuity themes and trends. The process model proposed by this guide covers four major steps:

- Business impact analysis
- Risk assessment
- Risk management (includes the development of a BCP)
- Risk monitoring and testing

\textsuperscript{3} More information can be found at \url{http://www.ffiec.gov/ffiecinfobase/index.html}. 

Page 37 of 49
It is interesting to note that this model presents the view of an integrated risk and business continuity management process. On the other hand, the process model is not as comprehensive as typical BCM frameworks and important elements are either missing or poorly developed (e.g. response prevention, planning, implementation).

For formal consideration in the analysis, preference was therefore given to the British FSA BCM Practice Guide.

3.5.4 Healthcare BCM

Business Continuity is also of major interest for the healthcare business. One international organisation working in this field is the BCPWHO: Business Continuity Planning Workgroup for Healthcare Organisations, the healthcare industry's membership organisation exclusively focused on providing leadership in the advancement of business continuity, disaster recovery and emergency management through collaboration and research. Founded in 2005 BCPWHO represents individual members from the healthcare industry across the United States, Canada and around the world⁴.

BCPWHO does however not promote any particular standard or guideline and no further equivalent international organisation has been identified under this study. For this reason, no example from the healthcare domain has been selected for further analysis.

⁴ More information can be found at http://www.bcpwho.org/.
4 Desktop Study – Comparative Analysis of Selected Standards and Guidelines

4.1 Holistic, general Standards and Guidelines

4.1.1 General Categorisation

For this group of criteria, the differentiating elements as identified on the basis of the analysed resources refer to:

- **Scope and underlying framework**: Differences in the underlying framework are the most distinctive feature of standards and guidelines. Strong similarities are found between all BCM-based resources, whereas others adopt a particular conceptual framework. This is the case for CMMI for Services (CMMI is a model for process improvement and only addresses key aspects of service continuity) and ANSI/NFPA 1600 (which places a stronger focus on disaster and emergency management). The scope of ISO/PAS 22399 and ASIS SPC.1-2009 is also slightly different from other BCM standards in that these rely on organisational resilience and Incident Preparedness and Operational (business) Continuity Management (IPOCM), for example some BCM standards are weak in the way they address incident prevention (see section 4.1.2).

- **Holistic approach**: Most standards may be categorised as being ‘holistic’ even though some differences can be found in the way the resources identify the BCM components or equivalent. One should consider though that virtual all standards and guidelines are generic in nature and have no fundamental limitations as concerns application to an organisation as a whole and all its processes.

No references for the application of these (or similar) general standards in the energy sector were found. This does of course not constitute any kind of proof regarding the way operators and other stakeholders in the energy supply chain adopt concepts of BCM, IPOCM and contingency management. The reader should consider here the overview of NERC standards and security guidelines presented in section 3.4.1.

4.1.2 Structural Elements

In the following a brief overview of the common elements and differences for each type of structural element is shown.

4.1.2.1 Programme Management

Most elements are common, however not all standards address legislative and regulatory constraints and requirements within the programme management.

4.1.2.2 Organisational Analysis

Standards and guidelines are similar, but there are also some variations in scope or level of detail:

- The core element is business impact analysis, including the identification of critical activities.
D2.2 Contingency Planning and Business Continuity Methodologies

- Continuity requirements are also in most standards and guidelines, particularly addressed in terms of maximum period of outage / disruption, recovery time objectives etc.

- Risk assessment and vulnerability analysis is another common element, but in some standards and guidelines it is weakly described and only implicit, probably because BCM and equivalent approaches are seen as integral part of a general risk management process.

- Choices are mostly addressed from the perspective of a cost-benefit analysis.

4.1.2.3 Components

All standards and guidelines recommend ‘typical components’ and these should by no means be seen as exclusive. From this perspective, some differences can be identified:

- External and interdependencies are often mentioned, but generally from the perspective of external conditions for the organisation’s own business continuity. Hence, the coordinated adoption of BCM concepts and principles by interconnected operators, service providers etc. is out of the scope of the current standards and guidelines.

- The impact on the environment is often not mentioned, but this aspect should be seen in the context of regulatory obligations addressing environmental pollution.

- In the category for ‘other’ components, some additional relevant aspects are mentioned, including the organisation’s image and reputation as well as economical and financial issues.

4.1.2.4 Development and Response Implementation

In this category of criteria, the differences in scope become more apparent:

- The most significant difference is that a number of standards place the focus only on incident response processes, but not on prevention processes (fully addressed only by ISO/PAS 22399 and ANSI/NFPA 1600).

- Response plans usually address the three dimensions: incident / emergency, continuity and recovery. However, the scope of the mandatory or recommended plans is not always fully clarified and/or matched with the identified criteria for analysis (e.g. recovery only mentioned as part of response management or continuity, emergency preparedness covered only by the identification of emergency resources etc.).

- Business continuity is almost always separated from other response plans by means of a particular continuity plan.

4.1.2.5 Process Management

The conclusions are similar to Programme Management, i.e. references have most elements in common, but vary in detail or do not explicitly address some elements:

- Common elements cover maintenance and review processes.
Exercises are not specifically addressed by AS HB 221:2004 and CMMI, but they are present in all other standards and guidelines.

Performance and self-assessment is not addressed by all standards with the same level of detail, and if often ‘diluted’ in the provisions on reviewing.

A similar consideration can be made with regard to continuous improvement; some standards mention only corrective actions rather than a systematic management approach focused on continuous improvement and development.

4.1.2.6 Organisational Preparation and Culture

All references consider the two criteria for this category, with only slight variations in terms of the communication strategy:

- Training is considered in all standards.

- A communication strategy is considered by most standards and guidelines, however with some differences as concerns the creation of a new organisational culture and awareness by all members of an organisation (typical for ‘pure’ BCM standards) as opposed to communication to directly involved staff (project team etc.) only. Most standard also consider external communication to stakeholders, the public, media etc.

4.2 Sector and Domain-specific Standards and Guidelines

4.2.1 General Categorisation

The differentiating elements as identified on the basis of the analysed resources refer to:

- Scope and underlying framework: The scope and underlying purpose of the analysed standards and guidelines varies, turning a direct comparison more difficult. For example, ICT-related standards focus on mitigation and recovery aspects, whereas financial guidelines were found to address BCM in general, even though with identified shortcomings.

- Holistic approach: These standards and guides are by default not holistic.

4.2.2 Structural Elements

4.2.2.1 Programme Management

The common criteria for programme management are generally met, however for some elements not as explicitly as for the holistic standards (e.g. strategy/policy definition).

4.2.2.2 Organisational Analysis

In line with holistic standards and guidelines, risk assessment and impact analysis are central elements present in all references. Conceptual differences are summarised as follows:
• Impact analysis is mandatory, but in general more focused on critical assets (e.g. ICT infrastructure) or specific functions (e.g. transactions) rather than organisational processes and functions. Risk assessment and vulnerability analysis are considered (at least implicitly).

• The definition of continuity requirements is similar to holistic BCM standards and guidelines; one exception is ISO/IEC 25762 that does demand a management process that formally includes these requirements (maximum outage time).

4.2.2.3 Components
Standards and guidelines do consider all key BCM components (people, assets / infrastructure, information and continuity). Due to their specific scope, only the environment is not indicated in any of the analysed resources.

4.2.2.4 Development and Response Implementation
The conformance with the criteria varies between the analysed standards and guides; the differences are explained by variations in scope and purpose:

• Only recovery is strongly addressed by all resources.

• Risk mitigation and other preventive measures are covered by ICT-related standards and guides and emergency preparedness is weakly addressed. On the other hand, the financial guides are more concerned with continuity aspects.

4.2.2.5 Process Management
These are weaker than the holistic standards in the way they address process management in general and for particular elements. This leads to the conclusion that standards and guides are comparatively weak in the way they address performance assessment and continuous improvement. However maintenance and review is considered by all references, but with less emphasis for the financial guide.

Testing (including exercising) is the only common element found in all references.

4.2.2.6 Organisational Preparation and Culture
The conclusions here are similar to the considerations for holistic standards and guidelines:

• Training is considered by all references.

• Communication is considered as well; in comparison to holistic standards, the scope of communication is more limited (to team level, for staff directly involved in the implementation of plans at operational level), for example the objective of creating a particular organisational culture is not reflected.
5 Conclusions

5.1 Synthesis of the Analysis

5.1.1 Matrix of Criteria vs. Standards

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Guideline</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Holistic approach</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Energy sector</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>International</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>n/a</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Framework</td>
<td>IPOCM</td>
<td>underlying CMMI framework</td>
<td>BCM system, PDCA cycle</td>
<td>BCM system, PDCA cycle</td>
<td>particular BCM management process</td>
<td>OR Management System, similar to IPOCM</td>
</tr>
<tr>
<td>Structural Elements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programme Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsibilities</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Documentation</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Strategy / Policy</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Regulation</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Organisational Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIA</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Critical activities</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Continuity requirements</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Risk &amp; Vulnerability</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Choices</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Components</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>People</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Information</td>
<td>partial</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>External dependencies</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Environment</td>
<td>yes</td>
<td>no</td>
<td>partial</td>
<td>partial</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Continuity</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Development &amp; Response Implementation</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>partial</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Emergency preparedness</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Business continuity</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Response management</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Recovery</td>
<td>yes</td>
<td>partial</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Process Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance assessment</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Exercising</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Maintenance and review</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Continuous improvement</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
</tr>
<tr>
<td>Organisational Preparation and Culture</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Communication</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Training</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
### General Categorization

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Guideline</td>
<td>partial</td>
<td>no</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
</tr>
<tr>
<td>Holistic approach</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Energy sector</td>
<td>no</td>
<td>no</td>
<td>see DOE CIO CS-7</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>International</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Framework</td>
<td>particular programme structure</td>
<td>BCM, PDCA</td>
<td>contingency planning process</td>
<td>ICT DR service provision framework, DR planning approach</td>
<td>based on BCM, but presented as process</td>
</tr>
</tbody>
</table>

### Structural Elements

#### Programme Management

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibilities</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
</tr>
<tr>
<td>Documentation</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Strategy / Policy</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Regulation</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

#### Organisational Analysis

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BIA</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>partial</td>
</tr>
<tr>
<td>Critical activities</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Continuity requirements</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Risk &amp; Vulnerability</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>partial</td>
<td>yes</td>
</tr>
<tr>
<td>Choices</td>
<td>partial</td>
<td>yes</td>
<td>partial</td>
<td>no</td>
<td>no</td>
</tr>
</tbody>
</table>

#### Components

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Information</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>External dependencies</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>partial</td>
<td>yes</td>
</tr>
<tr>
<td>Environment</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Continuity</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>

#### Development & Response Implementation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident prevention</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>no</td>
</tr>
<tr>
<td>Emergency preparedness</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>partial</td>
<td>no</td>
</tr>
<tr>
<td>Business continuity</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Response management</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>partial</td>
<td>yes</td>
</tr>
<tr>
<td>Recovery</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

#### Process Management

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance assessment</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>partial</td>
<td>partial</td>
</tr>
<tr>
<td>Exercising</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Maintenance and review</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Continuous improvement</td>
<td>partial</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>partial</td>
</tr>
</tbody>
</table>

#### Organisational Preparation and Culture

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>partial</td>
<td>yes</td>
<td>partial</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Training</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 2: Matrix for Criteria vs. Standards and Guidelines

Table 1 shows the synthesis of the analysis in terms of the level of compliance of each standard and guideline with respect to the analysis criteria. The level of compliance is indicated in three fundamental levels:

- Yes: The standard or guideline matches the criteria, the structural element can be clearly identified. There may be variations though with regard to the level of detail of the given description, explanations etc.
• **Partial**: The match with the given criteria or with the structural element is either ambiguous or weak. This includes cases where it was considered that the match is ‘implicit’, the criteria is only superficially addressed and not well identified.

• **No**: The match with the given criteria or with the structural element cannot be identified.

This analysis only provides a limited view on the differences between the standards and guidelines and just helps to identify potential strong points and shortcomings of the latter. In order to obtain a better insight, a Microsoft Excel Spreadsheet with a more detailed description of conclusions for each single element (specific criteria for a standard or guideline under analysis) is provided as annex to this report.

### 5.1.2 Common Elements and Conceptual Differences

As discussed in section 4, the holistic BCM standards and guidelines have most of the selected criteria in common. This is not surprising as many references refer to each other and the groups of authors for one standard certainly accompany the development of others. In other words, the BCM area is quite mature in the way standards and guidelines are currently specified and described.

The most common elements identified in virtually all references are Business Impact Analysis (BIA) associated with the identification of critical processes and resources. From this analysis, specific continuity objectives and requirements (maximum outage times etc.) are derived in most cases, and based on these a set of plans for continuity, emergency response, recovery etc. is developed.

Differences found were mostly due to variances in the main scope of the standard or guideline, for example incident prevention is not dealt with in the same way or with the same level of detail by all references. It should be mentioned here that ISO/PAS 22399 and ASIS SPC.1-2009 follow a slightly different model (IPOCM, OR Management System, respectively); these models are similar to, but not identical with other BCM references and pay more attention to incident prevention.

From a general perspective, BCM has to be seen in relation to other management systems and supporting standards and other documentary sources. In particular for risk assessment and vulnerability analysis, one should consider that some references presume a synchronised risk management process that already provides all required risk information. Differences were also found in the level of detail of specifications and guidance for implementation.

Detailed specifications support a tick-box approach for the verification of compliance, but this is not sufficient enough to guide organisations (in particular the inexperienced ones) through a formal implementation process. A number of standards or guidelines provide templates or suggestions for the structure and content of key documents (e.g. BC plan, response plan).

Domain-specific standards and guides may formally match many or most of the analysis criteria; however care should be taken when making a comparative analysis to BCM standards and methodologies, as they use to focus on domain-specific continuity aspects only. These references are weaker than the holistic standards in the way they address process management in general and for particular elements such as performance assessment and continuous improvement.
5.2 Outlook for the EURACOM Contingency Planning Approach

The analysis demonstrates the maturity of available BCM standards and guidelines and underlying BCM frameworks and process models. From this point of view, there is little doubt that a common approach for contingency planning under EURACOM (i.e. for application to energy infrastructures) should incorporate the critical, common elements of these existing models, i.e. integrated with a common approach for risk and vulnerability assessment as well.

Even though a more detailed view on the specific requirements for energy infrastructures (i.e. for contingency/business continuity) were not yet available the time of the analysis and the writing of this report, it is possible though to identify some fundamental shortcomings that a common EURACOM approach should overcome in order to ensure its suitability for the targeted purpose.

− Holistic BCM standards and guidelines provide an adequate framework, however should be tailored to the needs of the sector. This tailoring should for example adequately consider typical threats and vulnerabilities and requirements and objectives for continuity of operations.

− The interconnectivity of networks and their dependencies are key issues for EURACOM. Even though BCM standards and guides mention the need to address external dependencies, the focus is always on the continuity of the own organisation. So the question is: how could BCM be applied to interconnected networks (in a coordinated manner several operators at the same time)?

− The last point also impacts on the way interconnectivity related incidents are documented, reported, jointly analysed etc., how joint exercising, maintenance and review is organised, allowing for a continuous improvement of the established practices.

− The common approach should propose tools and methods tailored to the purpose of the analysis, e.g. for risk assessment, impact analysis, definition of continuity requirements, incident prevention and response etc., providing guidance for the adoption and execution of the proposed approach.
D2.2 Contingency Planning and Business Continuity Methodologies

References


EURACOM. D1.1: *Generic system architecture with relevant functionalities for hazard identification*, draft, October 2009.

EURACOM. D2.1: *Common areas of risk assessment methodologies*, draft. October 2009


ISO. *ISO/IEC 24762, Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services*. 2008


ANNEX

Excel file: EuracomD2.2_analysis.xls
<THIS PAGE IS INTENTIONALLY BLANK>