System View of Business Continuity Management

Vlasta Svata

Department of Systems Analysis

University of Economics, Prague, Czech Republic

svata@vse.cz

Abstract: *We are living in time where the impact on continuity still grows both on the side our personal lives and business activities. In the same time different international, regional, national, state and private organizations initiated to provide different actions and regulations in order to find the best solutions of this situation. The result is that there exist the whole set of different views over this problem. The main aim of this article is to map this situation, to provide the general framework of business continuity management (BCM) and to discuss its main parts and their mutual relationships. Special impact is given to the integration of the business and IT oriented solutions and ways of assurance initiatives helping managers to assess the implemented solutions and their compliance to the business strategy and other existing regulations.*

Key words: Business Continuity Management (BCM), IT Continuity Management (ITCM), business risk management, IT risk management, Business Impact Analysis (BIA), disaster recovery plan, business continuity plan, certification audit, non-certification audit

1. Introduction

All the time it is evident, that the main aim of all business activities in general is to produce different types of values to different types of stakeholders. Every event having negative impact on final business values is viewed as disruptive and management is accountable for the development of control system which should predict, prevent, detect, reduce or correct the harmful events. According to research by the META Group, the potential financial loss due to downtime is staggering. For an online retailer, the hourly loss is over one million dollars, on average. For a financial institution, the average hourly loss is closer to $1.5 million. And for utility companies such as telecommunications and energy, the potential loss can reach as high as $2.8 million per hour. That's over $67 million in a day or $24.5 billion per year (Societal Security, 2013).

In the same time it is clear, that there exist unimaginable number of events that have potential to disrupt the business processes together with the whole set of controls that can help managers to solve this problem. With the growing reliability of business on IT the specific attention is given to the technological events and controls. Therefore in past (during the 1980s and early 1990s) contingency planning and disaster recovery were largely information technology-led. But there was a growing recognition that this needed to become a business-led process and encompass preparing for many forms of disruption. In light of this, the discipline became known as business continuity management (BCM). When implementing BPM we have to challenge to find the right balance between the costs of control systems and potential impact of disruptive events. Therefore there exist many different regulations aiming to help managers to do this difficult job. Furthermore in case, that control system is in place, an independent and objective assessment of such a control is needed. In this case different types of audit/assurance activities are viewed as the best practice.

The main aim of the paper is to discuss:

- Different types of loss events
- The content and core parts of business continuity management and their mutual relationships (BCM Framework)
- Regulations relevant for BCM implementation
- Types BCM audit/assurance activities and related regulations.

2. Types of Loss Events

Today's society becomes ever more rapidly vulnerable to the different types of loss events. Basically the loss events are used to be categorized according two different aspects:

1. Aspect of the loss event enabler
2. Aspect of the loss event size

Applying the first aspect, there exist the following types of disaster categories:

- Natural disasters which are accelerated by the concentration of populations in mega-cities
  - Weather related (flooding, fire/wildfire, hurricane, heat/drought, thunderstorm / tornado, winter storms)
  - Geology related (Earthquake, Landslide, Volcano, Tsunami)
  - Public-health (epidemic / pandemic)
- Technological disasters: electric power supply breakdown
- Conflict based disaster: terrorist attacks, war, riot,
- Human systems failure: fire, plane crash
- Man-made: biological, chemical, , radiological, nuclear, explosive, terrorism
- IT related.

IT related loss events are used to be divided into

- Logical disasters
- Physical disasters.

Tab. 1: The relationship between the types of loss events, level of awareness and IT support.

Types of loss events	Level of awareness	IT Support	
		Methodological	**Technical**
Incident	Enterprise (internal)	Business and IT Continuity Management	• Traditional file-based backup and restore • Image based backup and restore • Bare metal backup and restore • Point in time snapshots • Data replication • Continuous Data Protection (CDP) • Local high availability (HA) configurations • Remote business continuity (hot standby) • Hosted or cloud based backup • Recovery to hosted/cloud based services • Managed DR services • Virtualisation enabled recovery
Emergency	Enterprise (internal) together with national or international (external)		

Disaster		Integrated protection system
		Crisis management
		Early warning systems
		Legal support
			• GIS and remote sensing
			  ○ Drought
			  ○ Earthquake
			  ○ Flood
			  ○ Landslides
			  ○ Search and rescue
			• Internet
			• Forecasting systems (flood, cyclone, stock exchange...)

Crisis	National or international (external)		

The second aspect for loss events categorization primary takes in account the value of loss. The most general term for the “agent” which activates unusual operations and can compromise the different values of an organization is event. But in the same time we often use terms like emergency, incident,

disaster or crisis interchangeably in many occasion. But in fact they have different meaning. (BCMI 2012) recognizes next types of loss events:

- An **incident** is an occurrence by chance or due to a combination of unforeseen circumstances, which, if not handled in an appropriate manner, can escalate into an emergency or disaster or crisis.
- An **emergency** is a sudden, unexpected event requiring immediate action due to its potential threat to health and safety, the environment, or property. When we have an emergency, it can be an incident however, the characteristics of this incident requires an immediate response as the situation do not permit the responder any time to wait.
- A **disaster** is a sudden unplanned event that causes great damage or serious loss to an organization. It results in an organization failing to provide critical business functions for some predetermined minimum period of time. It is common to distinguish natural, technological and social disasters, or natural and accidental.
- A **crisis** is a critical event that may impact not only profitability, reputation, or ability to operate
- of many organizations, but it negatively implies the lives of many people. It may not be time dependent and usually does not deny access to facility and infrastructure.

Except the attempts to distinguish between the different types of loss events, there exist different levels of disasters prevention and countermeasures (personal, business, IT, municipal, state, regional,…).

We can conclude that the position of IT within the business continuity management has two different faces. The first one resides in the fact, that the number and impacts of IT related loss events are still growing because of the growing dependence of business processes on IT. In the same time IT can help organizations to prevent, detect and restore business processes. IT thus can be both the driver and countermeasure for different types of loss events.

3. Business Continuity Management Framework

Even to the fact, that we basically understand the meaning and importance of BCM, going through the relevant literature we can conclude, that there is no common definition of this term and even more there is no unified opinion what it should encompass. Next are examples of some definitions:

- BCM is the “holistic management process that identifies potential threats to an organization and the impacts to business operation that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities” (Societal Security 2013)
- BCM is the development of strategies, plans, and actions to protect or provide an alternative mode of operations for business processes that, if interrupted, could seriously damage or cause fatal losses to an organization. It includes BCP, DR and crisis management (Mark, 2008).
- Business Continuity Management is a management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stake holders, reputation, brand and value creating activities (What is, 2013).
- BCM is implied as an organization-wide discipline and a complete set of processes that identifies potential impacts which threaten an organization. It provides a capability for an effective response that safeguards the interests of its major stakeholders and reputation (BCMPedia, 2013).

According to (ISACA Emerging Trends, 2012) BCM is an established component of risk management in many enterprises, and a common practice within BCM is to conduct business impact analysis (BIA) periodically or every time a significant change occurs within the enterprise. The key components of BCM are

- Disaster Recovery Plan (see later)
- Crisis management (CM)—Defines the steps necessary to address and mitigate the effect of a negative event, often while the event is still happening (e.g., fire, tornado, earthquake, severe weather)

- Incident response management (IRM)—Defines the necessary steps to address and minimize the negative impact of a physical or logical incident threating enterprise resources (people, physical and logical assets), e.g., theft, security breach or natural disasters
- Contingency planning—Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances
- Business Impact Analysis (see later).

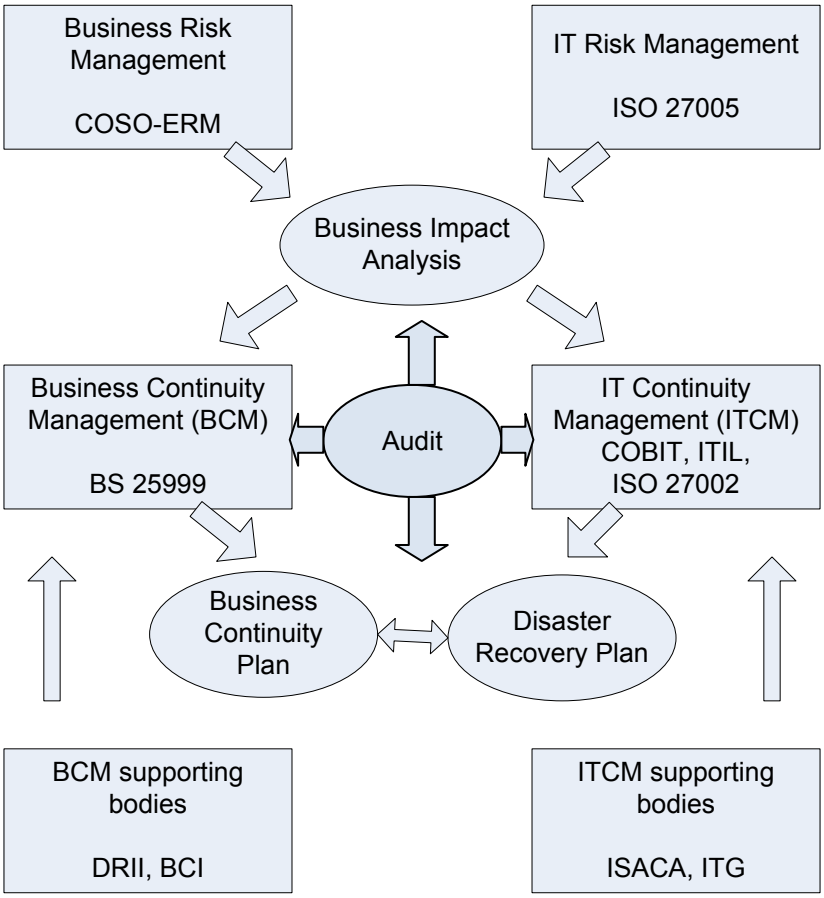

Fig. 1: BCM framework

More detailed description of BPM focuses in general on the next important issues:

- IT is an important part of business continuity management
- Risk management is the precondition for effective BCM
- The core documents of BCM are business continuity plan (BCP) and disaster recovery plan (DRP).

BCM is thus an umbrella which covers the whole set of different activities and documents. Fig. 1 is reaction on this situation and its main aim is to focus on the core parts of BCM and their mutual relationships. The framework distinguishes between management activities (Business Risk Management, IT Risk Management, Business Continuity Management, IT Continuity Management), the documents (Business Impact Analysis, Business Continuity plan and Disaster recovery Plan), regulations (COSO ERM, ISO norm, etc.) and assurance activities (audit, review).

4. BCM Related Management Activities

4.1 IT Continuity Management

IT Continuity Management (ITCM) draws upon a set of established business continuity processes to help ensure that IT systems supporting essential business functions remain functioning. ITCM ensures continuous operations of business applications and supporting IT systems (i.e., desktops,

printers, network devices). It is an inherent part of BCM and other parts of IT management (Emergency Management/Incident Management, Continuity of Operations, IT Security Management, Disaster Recovery, IT Service Management, etc.). An essential output of ITCM is IT Continuity Plan and/or Disaster Recovery Plan. While IT Continuity Plan deals with controls which should be embedded into the operational and tactical IT management processes, Disaster Recovery Plan is a special document that is related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster.

ITCM is thus more general and more oriented towards the preventive actions covering the whole life-cycle of IT continuity controls (Plan – Do – Check – Act) while disaster management is one part of ITCM which is oriented towards the specific more rare situations and their technological solutions.

4.2 Business Risk Management

Business risk management is in some literature replaced by the term Enterprise Risk management (ERM). (ISACA Risk IT, 2009) specifies ERM as the discipline " by which an enterprise in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the enterprise´s short- and long-term value to its stakeholders". Another relevant document COSO (COSO, 2004) 0defines "ERM is a process, effected by an entity´s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives".

There exist different components of the enterprise risk universe, as shown in Fig. 2.

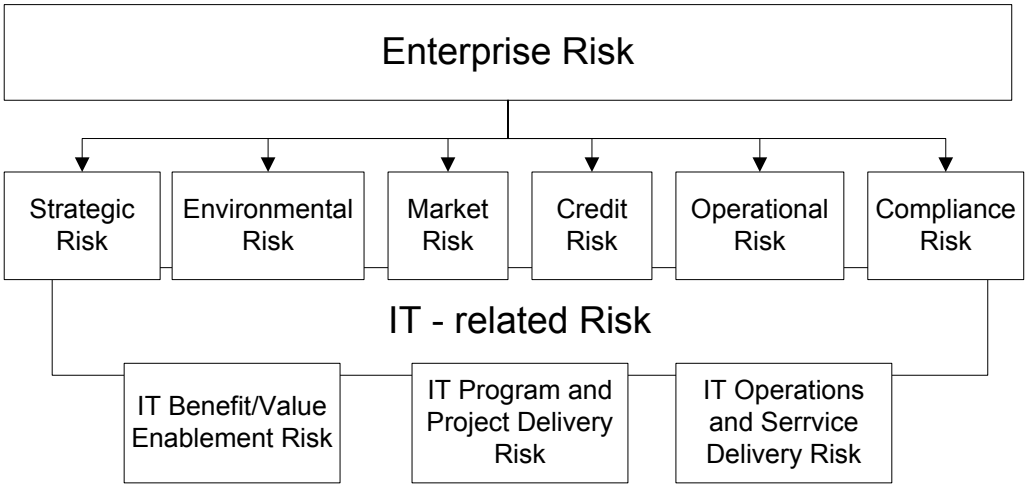

Fig. 2: Types of enterprise risk (ISACA Risk IT, 2009)

The core components of enterprise risk are: strategic risk, environmental risk, market risk, credit risk, operational risk and compliance risk. Information systems and/or information technology (IT-related) risk has entirely exceptional role within each organization.

4.3 IT Risk Management

IS/IT deals with the data/ information processing and as such managing IS/IT risk we are reducing the likelihood of "low quality" information. In the same time we are improving the quality of business processes, as information is the core part of each business process. Based on this assumption we can conclude that there is no need to make difference between the enterprise (business risk) and IS/IT risk. According to (ITGI, 2009), "IT risk is business risk – specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. The business value and IT risk are two sides of the same coin and risk is inherent to all enterprises"[1]. So there is the need to manage all the risks. But going through the frameworks, tools and documents dealing with risk and related continuity management, we came to the conclusion, that there is still gap between the "business" and "IT" area.

[1]Sometimes IT risk is considered to be component of the operational risk mainly in the financial industry in the Basel II Framework.

The risk management is conducted by many groups within an organization to fulfil a variety of business and regulatory requirements. The various groups within the same organization often rely on the guidance from different professional organizations to provide a framework for conducting the risk assessment. As these professional organizations offer disparate approaches to the risk assessment they contribute to the jungle of risk information.

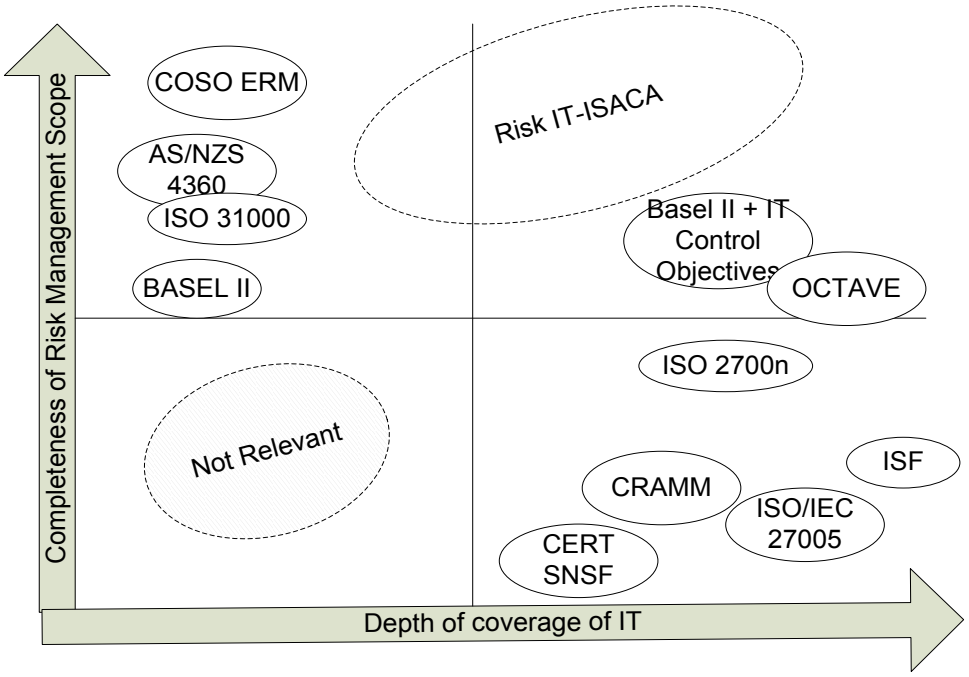

Fig. 3: Risk management frameworks (Svatá, Fleischmann, 2011)

Different types of risk assessment frameworks are shown in the Fig. 3. Their positioning within the axis X – Depth of coverage of IT and axis Y – Completeness of risk management scope can help us to understand both their relevance to IT/IS area and the level of commonness in the understanding the phenomenon of risk. We can summarize, that there exist the whole range of different frameworks dealing with the risk assessment, but these regulations either are too generic to be applicable for the IT risk management or although they deal with the IS/IT risk management, they are narrowing this area to the IT security risk management. The area named "Risk IT- ISACA" refers the only methodology Risk IT which complements ISACA´s COBIT. It provides a comprehensive framework for the control and - governance of business-driven, IT based solutions and services and thus attempts to bridge the gap between the business risk oriented frameworks and IT security risk management frameworks[2].

5. BCM Documents

5.1 Business Impact Analysis

The Business Impact Analysis (BIA) is the fundamental building-block for both the risk management and continuity management. It is a whole-of-business analysis that identifies critical resources and functions and the timeframes in which these must be restored following a disruption. This then allows realistic consideration of business recovery strategies. An impact analysis results in the differentiation between critical (urgent) and non-critical (non-urgent) organization functions/ processes. A function/process may be considered critical if the implications for stakeholders of damage to the organization are regarded as unacceptable. It may also be considered critical if dictated by law. Setting the barrier between the „acceptable" and „non acceptable" risks it is recommended to provide two parameters:

[2] For the more detailed description of the different risk management frameworks see (Svatá, Fleischmann, 2011)

- Risk appetite is the broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission.
- Risk tolerance is the acceptable variation relative to the achievement of an objective (and often is best measured in the same units as those used to measure the related objective.

The main outputs of BIA are the recovery requirements for each critical function/process. Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function (business portion of the recovery), and/or
- The technical requirements for recovery of the critical function (IT portion of the recovery).

They are expressed by the help of two values:

- Recovery Point Objective (RPO) - the acceptable latency of data that will be recovered
- Recovery Time Objective (RTO) - the acceptable amount of time to restore the function

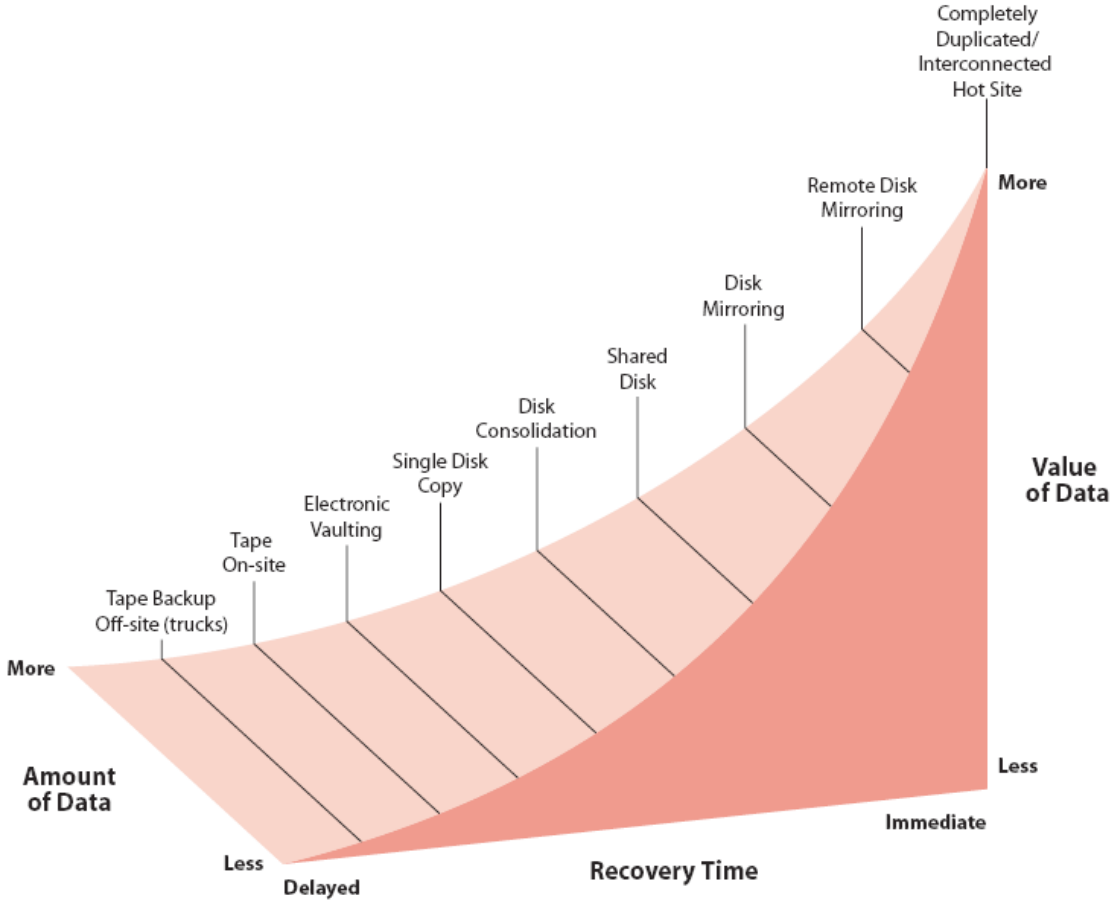

Fig. 4: Data types and disaster recovery (Schulman, 2004)

The Recovery Point Objective must ensure that the Maximum Tolerable Data Loss for each activity is not exceeded. The Recovery Time Objective must ensure that the Maximum Tolerable Period of Disruption (MTPD) for each activity is not exceeded.

Many solutions are available depending on the organization's recovery objectives. Each solution requires different costs and therefore it is important to provide balancing between the recovery objectives, value of data, amount of data and costs of solution. For example, when looking at RPO, one may be concerned with the cost of some data loss (typically less than five minutes, depending on the replication methodology). You may prefer having the ability to quickly perform a database restart instead of a no-data-loss option. Or, one may prioritize limiting possible impacts to the production environment and ensuring easy recovery (minimizing rolling disaster and database corruption) at the secondary site.

Most backup today are based on technology that is at least 40 years old (Quorum, 2012) even to the fact, that virtualization of servers, optimization of networks, and cloud storage are just a few new

technologies that have transformed the backup, recovery, and continuity solution landscape. It is expected , that enterprises will increasingly require automatic, tiered data protection that includes CDP[3], snapshots, D2D[4], tape, remote replication, and cloud. To stay cost-effective and to enable data managers to balance costs with recovery time and risk, data protection technologies will need to be capable of automatically identifying and moving low-priority data to the lowest cost recovery tier -- without administrator involvement.

After defining recovery requirements it is recommended to integrate them with the potential risks (threats) by the help of the risk scenarios. Risk scenario is a technique by which the different relevant and important risks are identified and their impact on business activities is assessed. This technique can be provided via two different mechanisms:

- A top-down approach, where one starts from the overall business objectives and related critical business activities (see output of the BIA),
- A bottom up approach, where a list of generic scenarios is used to define a set of more concrete and customized scenarios, applied to the individual enterprise situation.

5.2 Business Continuity Plan

A business continuity plan (BCP) is an enterprise wide group of processes and instructions to ensure the continuation of business processes in the event of an interruption. It provides the plans for the enterprise to recover from minor incidents (e.g., localized disruptions of business components) to major disruptions (e.g., fire, natural disasters, extended power failures, equipment and/or telecommunications failure). The plan is usually owned and managed by the business units and a disaster management or risk prevention function in the enterprise (ISACA, 2009).

According to ISO 22301, business continuity plan is defined as “documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.” (clause 3.5)

This basically means that BCP focuses on developing plans/procedures, but it doesn’t include the analysis that forms the basis of such planning, nor the means of maintaining such plans – all these are required elements of business continuity management that are necessary for enabling successful contingency planning.

Some regulations specify the requirements on the business continuity planning framework. On the base of these recommendations there exist the whole set or templates for such a document. The recommendations are very often complex making problems mainly smaller and midsize organizations. (Cosutic, 2012) recommends next optimal continuity plan structure for SME:

- Purpose, scope and users – why this plan is developed, its objectives, which parts of the organization it covers, and who should read it.
- Reference documents – to which documents does this plan relate? Normally, these are Business Continuity Policy, Business Impact Analysis, Business Continuity Strategy, etc.
- Assumptions – the prerequisites that need to exist in order for this plan to be effective.
- Roles and responsibilities – who will be responsible for managing the disruptive incident, and who is authorized to perform certain activities in case of a disruptive incident – e.g. activation of the plans, urgent purchases, communication with media, etc.
- Key contacts – contact details for persons who will participate in the execution of the business continuity plan – this is usually one of the annexes of the plan.
- Plan activation and deactivation – in which cases can the plan be activated, and the method of activation; which conditions need to exist to deactivate the plan.

[3] CDP (Continuous Data Protector) is a disk-based backup and recovery solution that provides comprehensive data protection functions such as mirroring, snapshots, journaling, remote replication, and automated disaster recovery (DR) from an application service , allowing IT administrators to meet business protection.

[4] D2D (disk-to-disk) means hard disks usage for their backups as well as their primary data. Typically this involves backing up to a dedicated disk-based appliance or a low-cost SATA array, but this time the disk is acting as disk, not as tape.

- Communication – which communication means will be used between different teams and with other interested parties during the disruptive incident. Who is in charge of communicating with each interested party, and the special rules of communication with media and government agencies.
- Incident response – how to react initially to an incident in order to reduce the damage – this is very often an annex to the main plan.
- Physical sites and transportation – which are the primary and alternative sites, where the assembly points are, and how to get from primary to alternative sites.
- Order of recovery for activities – list of all the activities, with precise Recovery Time Objective (RTO) for each.
- Recovery plans for activities – description of step-by-step actions and responsibilities for recovering manpower, facilities, infrastructure, software, information, and processes, including interdependencies and interactions with other activities and external interested parties – these are very often annexes to the main plan.

5.3 Disaster Recovery Plan

In section 3.1 we have already discussed the mutual relationship between the IT Continuity Management, IT Continuity Planning and Disaster Recovery Planning. We can summarize, that the definition of DRP varies as the views over this document differ. There exist three basic opinions:

- The first maintains that DRP and BCP have more or less the same meaning and the labelling difference has its roots in evolution. The older name DRP was substituted by the more advanced one – BCP.
- The second views DRP as the part of the BCP that focuses upon recovery from, principally, physical disasters.
- The third one declares that BCP should look at how to recover the business and DRP is about recovering IT infrastructure. This is mentioned not only in some of the blogs but also some of the institutes preach the same.

DRP comprises consistent actions to be undertaken prior to, during and subsequent to a disaster. A sound DRP is built from a comprehensive planning process, involving all of the enterprise business processes. Disaster recovery strategies include the use of alternate sites (hot, warm and cold sites), redundant data centres, reciprocal agreements, telecommunication links, disaster insurance, business impact analyses and legal liabilities (ISACA, 2005).

6. Regulations

Some research on the web and a visit to some of the popular business continuity sites can help us in building a little database (which is obviously not exhaustive). Displaying the number of documents on a time axis (based on date of first publication) led to the following diagram (Fig. 5).

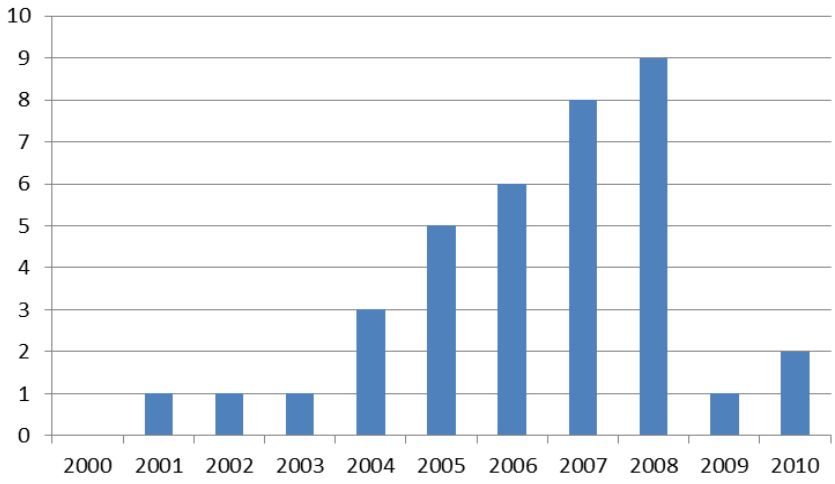

Fig. 5: The evolution of the number of BCM regulations (Verlinden, 2010)

In the period 2000-2003, industry specific bodies (such as Business Continuity Institute - BCI and Disaster Recovery Institute International - DRII) published their initial good practices and guides, which acted as a catalyst for other organizations. Amongst these we can find documents DRII PP - professional practices, or BCI GPG).

In the period 2004-2008, the growth in the number of regulations can find its origin in the publication of sector-specific guidelines/requirements (with the finance sector clearly leading the way) and the publication of some initial national standards, some of which are standards against which third party certification is possible

In the period 2007-2009, we can notice a great boom which was accelerated by the introduction of the international ISO standard on business continuity management (e.g. ISO/PAS 22399:2007). To the end of this period, the first standards regulating the BCM audit has been introduced (e.g. NFPA 1600 Business Continuity Management Audit Process).

Recently as an enterprise's vision and strategy change over time, it is important for all the involved roles and professionals to remain current on the various standards (e.g., ISO, NIST), frameworks (e.g., COBIT 5) and best practices that address BCM. These materials provide good references to support the establishment, maturity and assurance of specific BCM capabilities. Specific examples of these are:

- Standards such as:
    - International Organization for Standardization (ISO) 22301 Societal security -- Business continuity management systems --- Requirements, formerly BS25999—Business Continuity Management
    - Federal Financial Institutions Examination Council (FFIEC)—BCP Examiner's Handbook
    - NIST 800-34 Rev 1—Contingency Planning Guide for Federal Information Systems
    - ISO/IEC 24762:2008 'Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services.
    - ISO/IEC 27001 and 27002 - which is not primarily focused on ITCM, but on Information security Systems Management (ISMS).
    - ISO/IEC 27031 – Guidelines for information and communication technology readiness for business continuity
    - PAS 200 – Crisis management – Guidance and good practice
    - PD 25666 – Guidance on exercising and testing for continuity and contingency programmes
    - PD 25111 – Guidance on human aspects of business continuity
    - ISO/IEC 24762 – Guidelines for information and communications technology disaster recovery services
- Frameworks such as:
    - ISACA— Cobit 4.1, Cobit 5, Business Continuity Management Audit/Assurance Program, The IT Continuity Planning Audit/ Assurance Program,
    - The commercially developed Business Continuity Maturity Model (BCMM) for assessing state of preparedness
    - IT Infrastructure Library (ITIL)—Guidelines for The Business Continuity Planning Process and Documentation
- Best practices such as:
    - Business Continuity Institute (BCI)—Business Continuity Management-Good Practice Guidelines
    - Recovery Institute (DRII)—Business Continuity Planning Professional Practices
    - European Network and Information Security Agency (ENISA)—Business Continuity Management & Resilience.

Beside these internationally accepted regulations there exist the whole set of other standards which are country specific. Examples are:

- British Standards Institute: BS 25999, Parts 1 and 2
- PAS 56:2003 Guide to Business Continuity Management, British Standard
- National Fire Protection Association: NFPA 1600:2010

- Australia/New Zealand Standard AS/NZS 5050
- Singapore Standard SS540
- Canadian Standard: CSA Z1600
- Government of Japan BCP Guideline

Etc.

The core international regulation for BCM is ISO 22301. This standard has been developed by ISO/TC 223, Societal security. This technical committee develops standards for the protection of society from, and in response to, incidents, emergencies and disasters caused by intentional and unintentional human acts, natural hazards and technical failures. Its all-hazards perspective covers adaptive, proactive and reactive strategies in all phases before, during and after a disruptive incident. The area of societal security is multi-disciplinary and involves actors from both the public and private sectors. A challenge with ISO 22301 has been the large number of national documents on the subject, which has caused difficulties in gaining agreement.

The standard is divided into 10 main clauses, starting with scope, normative references, and terms and definitions. Following are the main clauses:

- Clause 4: Context of the organization
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

The committee has previously published the following standards and other documents:

- ISO 22300:2012, Societal security – Terminology
- ISO 22320:2011, Societal security – Emergency management – Requirements for incident response
- ISO/TR 22312:2011, Societal security – Technological capabilities
- ISO/PAS 22399:2007, Societal security – Guideline for incident preparedness and operational continuity management

The following projects are under development :

- ISO 22311, Societal security – Video-surveillance – Export interoperability
- ISO 22313, Societal security – Business continuity management systems – Guidance
- ISO 22315, Societal security – Mass evacuation
- ISO 22322, Societal security – Emergency management – Public warning
- ISO 22323, Organizational resilience management systems – Requirements with guidance for use
- ISO 22325, Societal security – Guidelines for emergency capability assessment for organizations
- ISO 22351, Societal security – Emergency management – Shared situation awareness
- ISO 22397, Societal security – Public Private Partnership – Guidelines to set up partnership agreements
- ISO 22398, Societal security – Guidelines for exercises and testing
- ISO 22324, Societal security – Emergency management – Colour-coded alert

We can conclude, that the main aim of the current stage in continuity regulation evolution is to provide consolidation of different national and professional regulation into one ISO family standards.

7. Audit

Last few years we can notice the trend to substitute the term audit by the term “assurance”. The objective of an assurance initiative is for an assurance professional to measure or evaluate a subject matter that is the responsibility of another party. For IT assurance initiatives, there is generally also a stakeholder involved who uses the subject matter but who has delegated operation and custodianship

of the subject matter to the responsible party. Hence, the stakeholder is the end customer of the evaluation and can approve the criteria of the evaluation with the responsible party and the assurance professional. The conclusion of the evaluation provides an opinion as to whether the subject matter meets the needs of the stakeholder (Svatá, 2011).

Current audit theories views audit as a specific type of assurance indicatives. 0An assurance professional may perform any of the following:

- Audit (certification or other)
- Review
- Agreed-upon procedures

Audit provides a high, but not absolute, level of assurance about the effectiveness of control procedures. This ordinarily is expressed as reasonable assurance in recognition of the fact that absolute assurance is rarely attainable due to such factors as the need for judgement, the use of testing, the inherent limitations of internal control and because much of the evidence available to the IT audit and assurance professional is persuasive rather than conclusive in nature. Specific type of audit is certification audit. The main aim of the certification audit is to provide assurance against the specified standard which includes and regulates this type of audit (e.g. ISO norm). The main output of a certification audit is not the final audit report, but certificate that the subject matter is compliant to the specific requirements. Certification audit can be provided only by those who are accredited by special accreditation bodies.

A review provides a moderate level of assurance about the effectiveness of control procedures. The level of assurance provided is less than that provided in an audit because the scope of the work is less extensive than that of an audit, and the nature, timing and extent of the procedures performed do not provide sufficient and appropriate audit evidence to enable the IT audit and assurance professional to express a positive opinion. The objective of a review is to enable the IT audit and assurance professional to state whether, on the basis of procedures, anything has come to the their attention that causes the IT audit and assurance professional to believe that the control procedures were not effective based on identified criteria (expression of negative assurance).

An agreed-upon procedures engagement does not result in the expression of any assurance by the IT audit and assurance professional. The audit and assurance professional is engaged to carry out specific procedures to meet the information needs of those parties who have agreed to the procedures to be performed. The IT audit/assurance professional issues a report of factual findings to those parties that have agreed to the procedures. The recipients form their own conclusions from this report because the audit and assurance professional has not determined the nature, timing and extent of procedures to be able to express any assurance (ISACA, 2010).

Focusing on BCM assurance, all the above mentioned types of assurance can be provided. The next text narrows the topic on the certification and other audits/assurance activities (non- certification).

7.1 Certification audit of BCM

The core regulation for certification audit of BCM is ISO 22301, the world's first international standard for Business Continuity Management (BCM). It is the new core international standard for Business Continuity Management System (BCMS) development and related certification audit.

BCMS is thus next management system which expands already defined management systems:

- ISO 9001: 2008 Quality management systems -- Requirements
- ISO 14001:2004 Environmental management systems -- Requirements with guidance for use
- ISO 20000:2011 Information technology – Service management
- ISO 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements.

The usual path for an organization that wishes to be certified against ISO 22301 is the following:

1. Implementation of the management system: Before being audited, a management system must be in operation for some time. Usually, the minimum time required by the certification bodies is 3 months.
2. Internal audit and review by top management: Before a management system can be certified, it must have had at least one internal audit report and one management review.

3. Selection of the certification body (registrar): Each organization can select the certification body (registrar) of its choice.
4. Pre-assessment audit (optional): An organization can choose to do a pre-audit to identify any possible gap between its current management system and the requirements of the standard.
5. Stage 1 audit: A conformity review of the design of the management system. The main objective is to verify that the management system is designed to meet the requirements of the standard(s) and the objectives of the organization. It is recommended that at least some portion of the Stage 1 audit be performed on-site at the organization's premises.
6. Stage 2 audit (On-site visit): The Stage 2 audit objective is to evaluate whether the declared management system conforms to all requirements of the standard, is actually being implemented in the organization and can support the organization in achieving its objectives. Stage 2 takes place at the site(s) of the organization's sites(s) where the management system is implemented.
7. Follow-up audit (optional): If the auditee has non-conformities that require additional audit before being certified, the auditor will perform a follow-up visit to validate only the action plans linked to the non-conformities (usually one day).
8. Confirmation of registration: If the organization is compliant with the conditions of the standard, the Registrar confirms the registration and publishes the certificate.
9. Continual improvement and surveillance audits: Once an organization is registered, surveillance activities are conducted by the Certification Body to ensure that the management system still complies with the standard. The surveillance activities must include on-site visits (at least 1/year) that allow verifying the conformity of the certified client's management system and can also include: investigations following a complaint, review of a website, a written request for follow-up, etc.

7.2 Other audit/assurance activities of BCM

The objectives of an non-certification BCM audit/ assurance review should provide management with:

- An evaluation of all above described parts of BCM framework separately and/or in their mutual relationships
- An evaluation of the BCM compliance to a desired regulations and business strategy
- An independent analysis of the effectiveness of the continuity plan
- An evaluation of the way to keep the continuity plans up-to-date.

For this purpose we can apply all above mentioned regulations internal organizational standards included. The planning and scoping phases of such an audit depends on the needs and requirements of stakeholders. While the BCM is regulated on the level of ISO standards, ITCM is regulated mainly at the level of best practices. The only exception is ISO 27002 Information technology -- Security techniques -- Code of practice for information security management. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. It contains best practices of control objectives and controls in the eleven areas of information security management. One of the area is business continuity management.

The best practices for providing non-certification audit/assurance of ITCM are Cobit 4.1 or Cobit 5 and IT Continuity Planning Audit/ Assurance Program from ISACA.

Cobit 4.1 is a set of documents each of which has different purpose and all together represent the best practice for Enterprise Governance of IT. Focusing on the BCM most relevant process DS4 – Ensure Continuous Service for the purpose of BCM audit we can apply:

- Cobit Framework - Helps understand WHAT should be done for developing system of controls. In case of BCM it describes the control objectives, inputs, outputs, measures, activities, responsibilities and CMM for the process DS4.
- Cobit Control Practices: Guidance to Achieve Control Objectives for Successful ITG - Helps to understand HOW to implement control objectives in practice. The control objectives of the process DS4 are:
    - DS4.1 IT Continuity framework
    - DS4.2 IT Continuity plans

  - DS4.3 Critical IT resources
  - DS4.4 Maintenance of the IT continuity plan
  - DS4.5 Maintenance of IT continuity plan
  - DS4.6 IT Continuity plan training
  - DS4.7 Distribution of the IT continuity plan
  - DS4.8 IT services recovery and resumption
  - DS4.9 Offsite backup storage
  - DS4.10 Post-resumption review.
- IT Assurance Guide: Using Cobit - Provides steps and tests of audit itself. In case of process DS4 it covers the tests of control design, test of control outputs and recommendation how to document the impact of the potential control weaknesses.

Cobit 5: Enabling Processes represents the new version of Cobit Framework (version 4.1). Specific guidance on BCM is provided in the following COBIT 5 enabling processes:

- EDM03 Ensure Risk Optimization—Determine whether IT risk appetite is commensurate with business objectives and enterprise risk tolerance
- APO02 Manage Strategy—Determine whether the IT strategy is aligned with business objectives
- APO09 Manage Service Agreements—Determine whether IT services and service levels meet current and future enterprise needs
- APO10 Manage Suppliers—Determine whether IT has processes to minimize risk associated with non-performing suppliers
- APO12 Manage Risk—Determine whether the IT strategy supports business requirements to comply with external laws and regulations
- BAI04 Manage Availability and Capacity—Determine whether IT has the necessary processes to predict performance and capacity requirements to maintain availability
- BAI06 Mange Changes—Determine whether risk associated with IT changes is properly assessed and reflected in the continuity strategy
- DSS04 Manage Continuity—Determine whether appropriate plans exist to enable the business and IT to respond to incident and disruptions in order to continue operations of critical business functions

The description of the Cobit 5 enabling processes includes process goals and metrics, process practices (in previous version control objectives) responsibility for process practices, inputs and outputs of process practices.

IT assurance guides for Cobit 5 enabling processes are not available till now.

The IT Continuity Planning Audit/ Assurance Program from ISACA provide a comprehensive guide to the assurance professional to plan and execute a business continuity assessment. Comparing previous documents it is more detailed as it was developed entirely for the purpose of this specific audit. In the same time it includes references both to the most relevant parts of COSO and Cobit 4.

This document is part of the IT Assurance Framework (ITAF[5]). IT Continuity Audit/Assurance Program describes in detail the separate audit/assurance steps. Thus it helps auditors and assurance professionals to assess the maturity of the defined control objectives of the process. The problem is that it is ITCM focused and gives a little support for the complex audit both the BCM and ITCM controls.

Tab. 2 is a result of the analysis of the relevant documents describing the recommended controls separately for BCM and ITCM. It includes the examples of controls that are to be tested together in order to achieve a system, end-to-end based assessment of the BCM. The complex BCM system of controls covers six areas each of which includes examples of recommended controls. Controls should be tested in two steps: test the control design and test the control output.

[5] ITAF provides standards that are designed to be mandatory, and are the guiding principles under which the IT audit and assurance profession operates.

Tab. 2: Practical example of the BCM system of controls

Practical Example of the BCM Control System
1. Continuity Framework and Policy
1.1 Control: The business has established a business continuity task force/ committee/organization to establish and maintain a business continuity process.
1.2 Control: The business continuity function includes representatives from affected business areas and IT, and the responsibility for the business continuity function is assigned to business operations and not IT.
1.3 Control: Determine if the BCM function is actively involved in the establishment of business continuity policy.
1.3 Control: The mission statement and goals of the BCP team are in alignment with the enterprise's policies addressing business continuity.
1.4 Control: Business continuity management is a process within the ERM (Enterprise Risk Management)
2. Business Assessment of Contingency Planning Requirements
2.1 Control: Risk assessment and BIA methods are utilized to establish business interruption exposures, their probability and impact, and remediation alternatives.
2.2 Control: The BIA is updated, at least annually, by the business and support units.
2.3 Control: Recovery point objectives (RPOs) have been established to provide guidelines for the time required to restore or provide interim services.
2.4 Control: Identified risks are entered into an issue monitoring system for inclusion in a business continuity plan.
3. Integration of Business Continuity and IT Continuity Plans (ITCP), Documentation
3.1 Control: The ITCP is aligned with and supports the business continuity plan.
3.2 Control: The entire business continuity plan and ITCP are documented and available during a declared emergency.
3.3 Control: The entire business recovery plan and IT recovery plan are documented and available during a declared emergency.
4. IT Continuity Plan Development
4.1 Control: The communications components necessary to provide network access to the computing facilities are included in the ITCP.
4.2 Control: The hardware configuration and procurement plans provide for the ability to acquire and configure hardware within the interim period established in the BCP.
4.3 Control: The critical applications and supporting platforms have been identified, and the required software and data are available for interim processing and restoration, and are in alignment with the BCP.
4.4 Control: Data recovery procedures have been established and tested to ensure availability of data.
4.5 Control: Appropriate facilities have been identified and plans are in place to support the interim processing and restoration of computer operations according to the priorities established in the BCP.
4.6 Control: Staff responsibilities, notification, substitution, and access procedures are in place to permit the timely assembly of staff and the commencement of interim and/or restoration procedures.
4.7 Control: The recovery plan contains adequate details to permit noncorporate IT professionals to implement the recovery plan if staff members are not available. The plan also provides for damage assessment, thresholds and formal decision points for plan activation.
4.8 Control: Third-party vendors who execute business processes are included in the ITCP or a separate vendor-specific ITCP, and both approaches subscribe to the same policies, standards, guidelines and procedures as internally executed processes.
4.9 Control: The plan is distributed on a need-to-know basis, is securely stored in soft and hard copy, and can be obtained from multiple locations in the event that the primary storage location has been affected by the incident.

Practical Example of the BCM Control System
5. IT Continuity Plan Maintenance
5.1 Control: The ITCP is maintained through inclusion in the systems development methodology, routine review of plan components and linkage to BCP reviews and enhancements.
5.2 Control: The ITCP is reviewed as part of all applications and systems enhancements.
6.BCP and ITCP Testing
6.1 Control: Testing policies define test frequency, types of tests, use of situational drills and other recognized processes.
6.2 Control: The BCP and ITCP tests utilize situational drills where resources are not available for the test, or the circumstances of the test are modified unannounced to verify the recovery team's ability to adapt to unplanned situations.
6.3 Control: The results from the BCP and ITCP tests are documented and analysed to identify issues that require BCP revision, additional training or additional resources.
6.4 Control: Plan testing includes verification that the tests were completed within the intervals established in the BCP.
6.5 Control: The business continuity tests utilize situational drills where anticipated resources are not available for the test, or the circumstances of the test are modified unannounced to verify the recovery team's ability to adapt to unplanned situations.
6.6 Control: The ITCP is tested routinely, according to the policy, and the tests address the requirements within the BCP.

8. Conclusion

Recent events and natural disasters resulting in business disruptions around the world illustrate the importance of having a robust and mature business continuity management (BCM) program as part of the enterprise strategic planning process. BCM moves to the forefront each time the news reports a major catastrophe or other loss-event.

Continuity needs are unique to each enterprise; however, there are common considerations that should be followed when planning an initial BCM program or modifying an existing one to address changes within the enterprise and the external environment. This article attempts to provide a system view over the "continuity environment" trying to identify and shortly describe the main components it. For the future we can expect, that the growing impact of the main trends such as rapidly changing business environment, global operations, regulatory scrutiny, and emerging technologies (e.g. social networks, mobile facilities) will force all the BCM stakeholders to provide more consistent, standard and cost efficient solutions. Thus the BCMS will become to be as important as the other management systems.

Bibliography

BAAS, S., RAMASAMY, S., PRYCK, J., D., BATTISTA, F, 2008: Disaster risk managementsystems analysis. A guide book, Food and Agriculture Organization of the United Nations, Rome, ISSN 1684 8241. http://www.fao.org/docrep/011/i0304e/i0304e00.htm

BCM Institute's BCMpedia for Business Continuity, 2012, http://www.bcmpedia.org/wiki/Main_Page

BCMPedia.org, BCM , http://www.bcmpedia.org/wiki/Business_Continuity_Management_BCM_Glossary, January 2013

Business Continuity Management Audit/Assurance Program, ISACA, 2011, ISBN 978-1-60420-186-4

Business Continuity Management: Emerging Trends, ISACA Emerging Technology White Paper, December 2012, http://www.isaca.org/whitepapers

COSO, 2004, Enterprise Risk Management - Integrated Framework, Executive Summary

COSUTIC, D., 2012: Business continuity plan: How to structure it according to ISO 22301. http://blog.iso27001standard.com/tag/business-continuity-plans/

HILES, A., 2003, Business Continuity: Best Practices (2nd Edition), Rothstein Associates Inc. ISBN: 1931332223

ISACA, 2005, IS Auditing Guideline: G32 Business Continuity Plan Review From IT Perspective

ISACA, 2009, IT Continuity Planning Audit/Assurance Program, ISBN 978-1-60420-079-9

ISACA, 2010, IS Auditing Guideline: G20 Reporting

ISACA, 2011, Business Continuity Management Audit/Assurance Program, , ISBN 978-1-60420-186-4

ISACA, Risk IT Framework, (2009), ISBN 978-1-60420-111-6

ISO 22301, Societal Security, Business kontinuity Management Systems, Whitepaper, www.pecb.org, January 2013

ITGI, 2007, IT Assurance Guide Using Cobi, ISBN 1-933284-74-9

TOIGO, J. W., 2002, Disaster Recovery Planning: Preparing for the Unthinkable (3rd Edition), ISBN: 0130462829

EDMEAD, M. T., 2008, The IT Auditor´ s Role in business Continuity management, http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management/

Quorum, 2012, publication: Top 5 must know facts hen considering a backup, recovery and continuity investment, www.quorum.net

SCHULMAN, R., 2004, Disaster Recovery Issues and Solutions, white paper, http://www.hds.com/assets/pdf/wp_117_02_disaster_recovery.pdf

STIMSON, M., 2005, *Principal Consultant*, VEGA Group PLC, Risk Management as Part of the Business, white paper

SVATÁ, V., FLEISCHMANN, M., 2011, IS/IT Risk Management in Banking Industry, *Acta Oeconomica Pragensia*, Vol. 19, No. 3, p. 42—60, ISSN 0572-3043

SVATÁ, V., 2011, IS Audit Considerations in Respect of Current Economic Environment, *Journal of System Integration,* Vol.2, No 1: p. 12-20, ISSN 1804-2724

The Civil Contingencies Act , 2004, http://www.legislation.gov.uk/ukpga/2004/36/contents

VERLINDEN, W., 2010, A short tour of business continuity management standards, http://www.continuitycentral.com/feature0742.html

What is Business Continuity Management?, 2013, http://www.talkingbusinesscontinuity.com/starting/what-is-business-continuity-management.aspx

JEL Classification: H84, M15