Proceedings of FIKUSZ '13 Symposium for Young Researchers, 2013, 133-141 pp © The Author(s). Conference Proceedings compilation © Obuda University Keleti Faculty of Business and Management 2013. Published by Óbuda University http://kgk.uni-obuda.hu/fikusz

Information Security Management for SMEs: Implementating and Operating a Business Continuity Management System (BCMS) Using PDCA Cycle

Gergely Krisztián HORVÁTH, CISA CISM

IT security manager, Hungarian National Asset Management Inc.

University of Pécs, Faculty of Business and Economics, PhD School in Business Administration

gergely.horvath@ceentrum.hu

Abstract: Recent information security incidents and regulatory changes makes highlight the need of solid information security management. From a business perspective one way to be secure is to be able to operate continua hespecially for companies operating critical infrastructure elements. Business continuity management is the discipline that helps organizations to keep on operating in case of disruption or crisis. SMEs oftentimes lack the experience to establish such management systems, Therefore assistance to SMEs to implement and operate a business continuity management system (BCMS) aligned with the information security management system (ISMS) is highly appreciated. The article summarize the background to this topic and related Hungarian regulations, then major BCMS implementation and audit methodologies are discussed. Finally checklists and guidance is given to SMEs, based on professional literature and author's experience, in order to successfully implement a BCMS system and operate it according to business needs and regulatory requirements.

Keywords: Information security, Business continuity, management systems, BCP, CIIP,

1 Drivers to implement integrated business continuity management system for SMEs

1.1 Cyber security incidents are on the rise

Media covers cyber threats with great detail in the past few years: from stealing individuals bank accounts, and stealing industrial secrets, to attacks to critical infrastructures, major cyber threats materialize frequently. The result of these events are heavy financial losses (p.e. Diginotar declared bankcrupt in 2011), damaged reputation (p.e.RSA hack in 2011), and mistrust of clients (p.e.Sony Playstation hack, 2011).

1.2 Developments in corporate governance practices

Corporate governance is an established management discipline with rootes dating back to East India Company (1707). The regulation has evolved to include detailed requirements on internal control (f.e. SOX). In Hungary, the Budapest Stock Exchange (2004), and the the National Asset Management Inc (2013) issued localized version of Corporate Governance Codes. Currently there are projects on corporate governance capability assessments at major state-owned enterprises, to manage strategic business risks based on EU funded GOSPEL project's spin-off Trusted Business Partner. It covers information security practices as well, where the continuity of operation is a key factor.

1.3 ERM and Information security risk management practices

Enterprise risk management (COSO ERM) has become the primary tool for organizational risk management: ERM became a regulatory requirement of a well-controlled organization! COSO (2004) defines ERM as 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."

ISO/IEC 27005:2008 deals with information security risk management. Next year ISO/IEC 31000:2009 became the global standardized method for risk management. Eventually, various aspects of risk management converge to provide an integrated view of the risks affecting enterprise's objectives.

1.4 Regulatory changes

Regulators on International level, in the US, EU and Hungary as well adopted the risk management approach, major examples:

- International: Basel II/III regulates operational risk management[1],
- US Congress: Sarbanes-Oxley Act of 2002, section 404, contains a detailed section on internal control systems,
- EU: 7th Company directive[2]
- Hungary: Law on Critical infrastructure protection[3] (2012) and the government decree on implementing the CIIP law[4] (2013). New Law on Information protection in central and local governement organizations require strict information security practices to be adopted by governmental bodies.

1.5 Requirement of a major client

In this chapter I discuss the main factors that drive Hungarian SMEs to implement BCMS on interviews of information security professionals. If not driven by the owner of a SME, in Hungary, oftentimes the need for BCMS is driven by a major client from a regulated industry, such as financial services.

2 Business continuity management practices

Business Continuity Management (BCM) is a relatively new management discipline. It has become increasingly important as organizations are currently finding themselves in a fast changing environment where new risks emerge in an increasing pace.

During my research I use the definition of BCMS as set out in the international standard ISO/IEC 22301 (clause 3.4), because this is the most widely accepted definition: “Holistic management process that identifies potential threats to and organization and the impacts to business operations 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.”

Business continuity management allows an organization to react to an incident in an efficient, timely manner and recover critical business processes within established

[1] Bank for International Settlements (BIS)publications at http://www.bis.org/bcbs/publications.htm

[2] Seventh Council Directive 83/349/EEC of 13 June 1983

[3] Law on Critical infrastructure protection – Act CLXVI of 2012 – 2012. évi CLXVI. tv. a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről)

[4] Decree on implementing Act CLXVI of 2012 - 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

timeframes (RTO, RPO). Michelberger and Labodi (2012) illustrate the related timeframes in a graph:

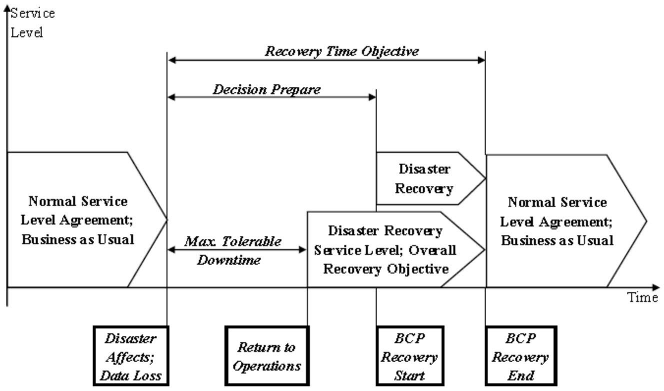
Service Level
Recovery Time Objective
Decision Prepare
Normal Service Level Agreement; Business as Usual
Max. Tolerable Downtime
Disaster Recovery
Disaster Recovery Service Level; Overall Recovery Objective
Normal Service Level Agreement; Business as Usual
Time
Disaster Affects; Data Loss
Return to Operations
BCP Recovery Start
BCP Recovery End

Figure 1
Business continuity model (Michelberger-Labodi, 2012, p4)

Disaster recovery (DR) is a term used for the process of preparation for the replacement of information systems following an incident. ITIL differentiate IT service continuity management (IT SCM) in the Service Design Book (ch. 4.5) which is broader than DR, and supports of the overall BCM process by ensuring that required IT facilities can be resumed within agreed timescales.

BCMS and IT SCM related international best practices are:

- ISO/IEC 22301:2012 is the first international standard on BCM,
- ISO/IEC 27031:2011 is an ICT-focused standard on IT SCM,
- NIST-800-34 (2010) is the US guide for Contingency Planning of federal information systems
- Cobit 5 for Information Security is the security view of the Cobit framework also covering continuity practices,

Information security governance is the responsibility of senior management, they provide strategic direction and resources. While information security management is the responsibility of information security managers and middle management. Their task is to implement and operate the ISMS. Related international best practices are:

- ISO/IEC 27000 series standards define ISMS requirement, where ISO 27031 define ICT continuity requirements.
- NIST – 800-39 (2011) federal guide gives advice on information security risk management.
- ISACA is the biggest IT governance and information security association, they have been publishing standards and guidelines for decades. Cobit 5 framework is the recent IT framework that covers information security.

3 Implementing integrated business continuity management systems for SMEs

3.1 Implementing BCMS as a project

Dr. W. Edwards Deming developped the cycle of control based on Walter A. Shewhart's statistical studies in 1951. This model is widely used in management systems to achieve continual improvement, the most notable examples are ISO 9001 quality management and ISO/IEC 27001 information security management standards and ISO/IEC 22301 standard also follows this logic therefore it ensures that it is consistent with other management system standards.

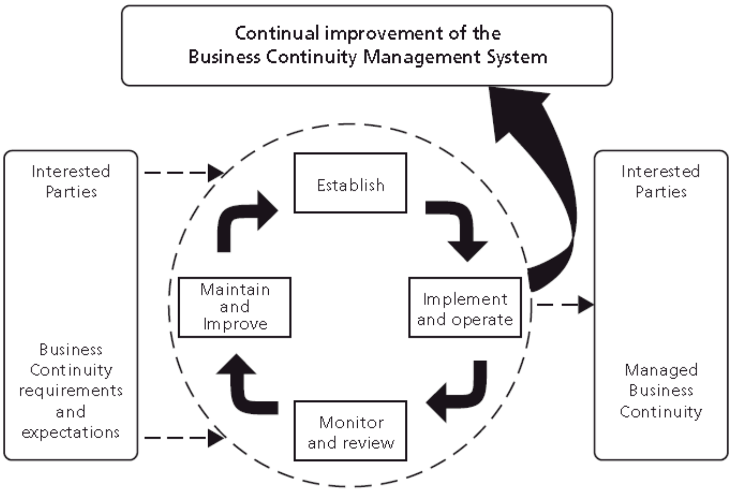
Continual improvement of the Business Continuity Management System
Interested Parties
Business Continuity requirements and expectations
Establish
Implement and operate
Monitor and review
Maintain and Improve
Interested Parties
Managed Business Continuity

Figure 2
Plan, Do, Check, Act cycle (source: BS 25999-2:2007)

The PDCA model in BCMS system produces business continuity outcomes that meet the requirements of interested parties. Related elements of a BCMS:

- **Plan**: Prepare BCM strategy, policy, objectives, processes and procedures in accordance with company policies and objectives.
- **Do**: Implement the BCM policy, processes and procedures and operate the BCMS system.
- **Check**: Monitor and review performance against BCM objectives, and report the results to management to authorize remediation and improvement actions.
- **Act**: Maintain and improve the BCMS.

3.2 Initiation and planning phase (PLAN)

It is important to define the business problem in their own terms as relevant to the SMEs business goals. It is advisable to define more steps to the solution so that it **can be implemented step by step** as resources are available to an SME.

Next, the **problem should be elaborated in more detail** specifying the exact requirements (business, compliance, IT, security, etc) of the BCMS project in harmony with management systems already in operation. Also important in this phase to analyse supporting ICT services and systems. The methodologies mentioned in chapter 2 of this article are used generally as a foundation.

In every business undertaking the knowledge of expectations and **preferences of stakeholders** helps in planning and also make the foundation for the success of the final acceptance test. Without senior management commitment the BCMS implementation is doomed to failure.

After proper planning it is advisable to **continue the work as a project** with designated project manager experienced in BCM implementation. The project has to have an organization, defined key roles, and **defined critical success factors**.

3.3 Desing and implementation phase (DO)

A methodology is generally not meant to be fully implemented for every process in a company, but careful scoping is required considering business needs and compliance requirements. It is highly advisable to select the international standard ISO 22301 as a foundation for BCMS, and use other BCM methodology elements where necessary and to integrate BCMS with other management systems. Integrated ISMS requires the following delivarables, integrated with a BCMS:

- Integrated ISMS and BCMS policy
- Security and BCM organization
- Assets classification and process impact assessment
- Standards, procedures and metrics

In design phase the project has to define elements of methodologies relevant to the organization. (methodology scoping), and define capability goals of related management processes. In case resources are not available to implement the whole scope in a single project it is important to prioritize requirements and phase the implementation.

First the tailored BCMS methodology and policies has to be prepared. The BCMS policy shall cover requirements, resources and organization.

All the roles detailed in methodologies are generally not possible delegate to separate people in an SME, so one must usually perform multiple roles to a colleague, but the roles can be merged only if they are not incompatible. The Head of Business Continuity shall be a manager with adequate skills and authority.

After the BCMS frameworks is ready, the next step is to define the most critical business processes by conducting a business impact analysis (BIA). Those processes shall be selected which have high impact on business goals, clients, turnover, or compliance. It is good practice to extend BCP plans gradually by major clients / products.

Next, a risk analysis shall be conducted to define high probability and high impact risk events. Based on risk analysis, management shall decide on risk response: transfer, avoid, reduce, or accept the risk. Usually BCP planning covers IT system loss, loss of office, unavailability of key personel.

Training of management and employees helps get their support in the planning and implementation phase as well. Key areas to cover in trainings:

- Why BCM is important,
- How do I get information about a crisis situation,
- What to do to in a crisis situation

It is important to continue doing trainings for new colleagues, and keep everyone informed with information updates, newsletters.

The final step in the implementation phase is BCP testing and acting on test results. Tests shall be detailed covering all major areas of the plan, such as a:

- call cascade to test communication details,
- walk through test, to verify plan details,
- possibly a simulation of most relevant risk scenarios to simulate real life cases

3.4 Monitoring and controlling phase (CHECK)

Senior management control of the implementation project keeps the momentum of BCM effort and keeps the project on track.

Also important to check compliance with initial project requirements and product quality, if possible by an independent professional.

After BCMS implementation project ends an internal or external auditor shall audit the BCMS and individual BCP plans.

3.5 Finalize and operate the BCMS and BCP plans (ACT)

The BCMS implementation is not a one time activity. The management systems has to be operated continously, and after major changes to business processes or supporting resources, IT systems, the plans have to be revised, re-trained, re-tested to ensure aplicability.

The real test of the BCMS is in case an incident happens how the organization react. It is expected that BCP plans minimize the impact of incidents to business and increase SME competitiveness.

In the PDCA cycle the improvement of BCMS is also considered to be in this phase: acting on management reviews, implementing improvement actions.

4. Conclusions

It is not straight forward for SMEs to implement international best management practices generally, it is even more so in case of business continuity management practices. Firstly, a methodology is generally not meant to be fully implemented for every process in a company, but careful scoping is required considering business needs and compliance requirements. Secondly, BCMS has to be integrated into the corporate governance structure and it has to be aligned and integrated with other management systems like ISMS. Finally, several important soft management factors need to be considered for the successful implementation of a BCMS.

Advantages of integrated ISMS and BCMS implementation include:

- Comprehensive and verifiable information security and business continuity strategy
- Information security and business continuity are transformed into a proactive activity
- Ensure compliance to existing and possibly future information security, and infrastructure protection related regulations
- Business alignment of information security activities
- Alignment with leading industry practices and methods

The article discusses related management best practices and provides a guideline to consider for executive management of SMEs on important factors before and while implementing a BCMS using best practices.

Subsequent research area could be to analyse the informations security and business conrinuity methods discussed in chapter 2 and link them with ISO 22301 to help implement coherent management systems (ISMS, BCMS).

Acknowledgement

I thank prof. Pál Michelberger for his motivation to continue publishing articles in my research area while working as a practicing information security manager. His advice and articles were very helpful.

And I thank for my wife and my family for the support they have given me while working on my PhD research topic: information security governance.

References

[1] Graham, J, Kaye, D: A risk management approach to business continuity: Aligning business continuity with corporate governance, Rothstein Associates, 2006

[2] Michelberger Pál - Lábodi Csaba: After Information Security - Before a Paradigm Change (A Complex Enterprise Security Model), Acta Polytechnica Hungarica, Vol 9., No. 4. 2012, ISSN 1785-8860, pp. 101-116

[3] Lábodi Csaba - Michelberger Pál: Necessity or challenge - Information security for small and medium enterprises, Annals of the University of Petrosani, Economics, Vol.X. part 3. ISSN 1582-5949, pp. 207-216

[4] http://en.wikipedia.org/wiki/DigiNotar

[5] COSO, Enterprise Risk Management—Integrated Framework Executive Summary, September 2004, (www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf)

[6] Hungarian National Asset Management Inc, Corporate Governance Guidelines, 2013 (http://www.mnv.hu/felso_menu/hireink/sajtoszoba/20130329.html?query=felel%C5%91s%20v%C3%A1llalatir%C3%A1ny%C3%ADt%C3%A1s)

[7] Budapest Stock Exchange, Corporate Governnce Recommendations, 2004 (http://bse.hu/data/cms61401/CGR_011212.doc.doc)

[8] Deming, W.E: Elementary Principles of the Statistical Control of Quality, JUSE, 1950

[9] ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements," 2005.

[10] www.mtaita.hu/hu/Publikaciok/ISACA_HU_COBIT_41_HUN_v13.pdf

[11] Cheffins, Brian R., The History of Corporate Governance (December 1, 2011). OXFORD HANDBOOK OF CORPORATE GOVERNANCE, Mike Wright, Donald Siegel, Kevin Keasey and Igor Filatotchev, eds., Oxford University Press, Forthcoming; University of Cambridge Faculty of Law Research Paper No. 54/2011; ECGI - Law Working Paper No. 184/2012. Available at SSRN: http://ssrn.com/abstract=1975404 or http://dx.doi.org/10.2139/ssrn.1975404