ITIL® and Information Security

Roman Jašek, Lukáš Králík and Miroslav Popelka

Tomas Bata University in Zlin, Faculty of Applied Informatics
NadStranemi 4511, 760 05 Zlin, Czech republic

Abstract. This paper discusses the context of ITIL framework and management of information security. It is therefore a summary study, where the first part is focused on the safety objectives in connection with the ITIL framework. First of all, there is a focus on ITIL process ISM (Information Security Management), its principle and system management. The conclusion is about link between standards, which are related to security, and ITIL framework.

Keywords: ITIL, ISM, Information Security, Information Security Management, ISO 20000, ISO 27000.
PACS: 07.05.Bx,

INTRODUCTION

Information security was in an earlier version of ITIL v2 included as a separate publication entitled Security Management. However in ITIL v3, the information security management (ISM - Information Security Management), is taken as a process. There it is defined as "a process that ensures the confidentiality, integrity and availability of assets of the organization, information, data and IT services. Information Security Management usually forms part of an organizational approach to safety management, which has a wider extent than just the operation of IT services, but it also applies to the handling of paper documents, access control systems, phones, etc., for the whole organization. "

Information Security Management within the ITIL v3 is comprehensively solved in the publication Service Design (Service Design) in 4.6 Information Security Management (Information Security Management). According to this methodology is the goal of Information Security Management is security of information technology and business processes to ensure the safety of all activities of management services.

PRINCIPLES OF ISM

ISM process should help to gather and process all problems and issues of information security. At the same time should ensure the creation, maintenance and enforcement of information security policy to include procedures for correct and incorrect use of all IT systems and services.

Security Policy

The security policy of the organization is one of the main pillars of information security management system. It is important to be clearly defined. Determines the framework for information security of organization, and after approval by the top management it is binding for all employees and other entities that are in contact with the ICT services of organization.

The security policy must be in accordance with the policy of the organization. It defines basic strategy, goals, attitudes, roles, responsibilities and principles regarding activities related to information security.

According to ITIL security policy includes:

- Policy of correct and incorrect handling of IT assets,
- Access control policy,
- Control policies passwords
- e-mail policy
- Internet Policy,
- Anti-virus policy
- Information classification policy,

Proceedings of the International Conference on Numerical Analysis and Applied Mathematics 2014 (ICNAAM-2014)
AIP Conf. Proc. 1648, 550020-1–550020-4; doi: 10.1063/1.4912775

- Policy document classification,
- Remote access policy,
- Policy to suppliers of IT services and components,
- Policy of disposing of the assets.

Information Security Management System (ISMS)

Information Security Management System is a well-known thing. ISMS is known for its comprehensive set of measures and requirements necessary to ensure the protection and security of information, know-how and assets of the company or institution in both the private and the public sector.

According to ITIL, ISMS provides the basis for the development of cost-effective for information security of program that supports the business objectives of the organization. This package includes the people, products and technologies, processes, partners and suppliers to ensure high levels of security.

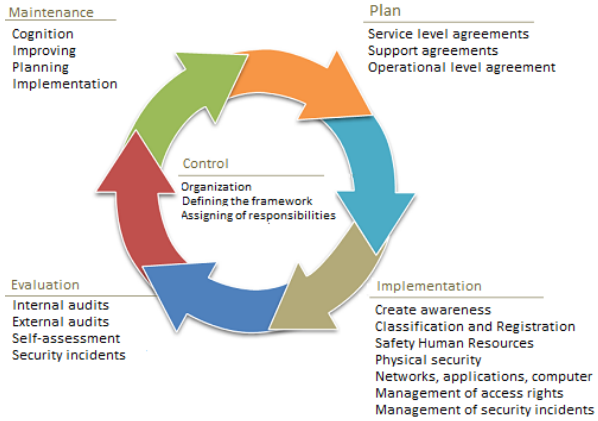

FIGURE 1. The basic framework for information security management according to ITIL

Control

The objective is to create a management framework to begin the process of information security and organizational structure for the preparation, approval and implementation of an information security policy. Also it is included the allocation of responsibilities and the creation of control of necessary documentation.

Plan

Planning focuses on the design and recommendation of appropriate security measures based on the requirements of the organization. These requirements are obtained from sources such as sales and service risks, plans and strategies, SLA (Service Level Agreements) and OLA (Operational Level Agreements), and the legal, moral and ethical responsibility for information security.

Implementation

The objective ISMS implementation is properly apply the appropriate processes, tools and control mechanisms to sufficiently support the security policy.

Evaluation

This point is the surveillance and control of compliance with security policies and security requirements of a regular audit of technical security of IT systems. In some cases, it can also provide information to external auditors and regulators.

Maintenance

This section is trying to improve the security agreement and improving the implementation of security measures and controls.

INFORMATION SECURITY STANDARDS

ISO/IEC 20000

It is an international standard in the field of ICT services. It is intended to carry out an objective independent certification audit of IT service management in the organization. If the service management system is in accordance with the requirements of the standard, then the certificate of compliance is issued to organization. This then ensures that the environment, in which services are provided, is managed and controlled. Thus are created organizational and technical requirements to ensure that services meet customer requirements for quality. The certificate is not in itself a guarantee of quality IT services. This standard has the same meaning as the well known standard ISO 9001, but this is focused on the entire enterprise while ISO 20000 focuses specifically on the environment of information systems.

This standard consists of five parts:

1) ISO/IEC 20000-1 – Information technology – Service management – Part 1: Specification,
2) ISO/IEC 20000-2 – Information technology – Service management – Part 2: Code of practice,
3) ISO/IEC TR 20000-3 – Information technology – Service management - Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1,
4) ISO/IEC TR 20000-4 – Information technology – Service management - Part 4: Process reference model,
5) ISO/IEC TR 20000-5 – Information technology – Service management – Part5: Exemplar implementation plan for ISO/IEC 20000-1.

Link between ISO/IEC 20000 and ITIL®

The standard ISO / IEC 20000 has a different purpose than the use of ITIL. Nevertheless complement each other. ITIL is a set of "best practices" in the area of service management. If it is implemented then it is helping to achieve the quality required by ISO / IEC 20,000. Consequently, the ITIL® is a framework for the design of processes required by this standard. The standard ISO / IEC 20000 presents clear objective requirements to verify that the "best practices" according to ITIL ® were actually applied, ie. Enables an independent certification service management processes.

ISO/IEC 27000

It is a group of international standards aimed at information security management in organizations (ISMS). This series of standards published since 2005.

ISO/IEC 27001

ISO / IEC 27001 is the main standard for Information Security Management System. Replaced BS 7799 and became the international standard of the field. It provides a comprehensive approach to information security in the organization. ISO / IEC 27001 include continuous improvement process of the entire information security management system using an integrated model of PDCA.

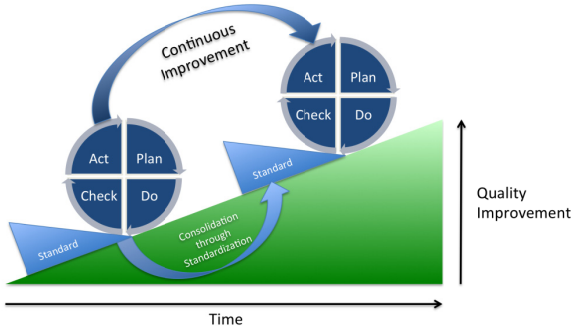

FIGURE 2. Model of PDCA cycle

ISO/IEC 27002

This standard is divided into 11 main areas. These areas contain a total of 39 categories of so-called security measures and 133. In each area are also specified their targets for the control of reach. In parentheses for each region are listed in the categories dedicated to safety.

- Security Policy,
- Organization Information Security,
- Asset Management,
- Human Resources Security,
- Physical and Environmental Security,
- Communications and Opertations Management,
- Access Control,
- Information Systems Aquisition Development and Maintenance,
- Information Securtity Incident Management,
- Business Continuity Management,
- Compliance.

ACKNOWLEDGMENTS

This work was supported by Internal Grant Agency of Tomas Bata University in Zlin under the project No. IGA/FAI/2014/020 and project No.IGA/FAI/2014/031.

REFERENCES

1. BUCKSTEEG, Martin. ITIL 2011. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.
2. ITIL continual service improvement [online]. 2nd ed. London: TSO, 2011, xi, 246 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331308-2. Dostupné z: http://www.best-management-practice.com
3. ITIL service transition [online]. 2nd ed. London: TSO, 2011, xii, 347 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331306-8. Dostupné z: http://www.best-management-practice.com
4. ITIL service design [online]. 2nd ed. London: TSO, 2011, xi, 442 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331305-1. Dostupné z: http://www.best-management-practice.com
5. ITIL service operation [online]. 2nd ed. London: TSO, 2011, xi, 370 s. [cit. 2013-07-22]. Best Management Practice. ISBN 978-0-11-331307-5. Dostupné z: http://www.best-management-practice.com
6. ITIL: service strategy [online]. London: Stationery Office, 2011, xii, 264 s. [cit. 2013-07-22]. ISBN 978-011-3310-456. Dostupné z: http://www.best-management-practice.com/
7. ISO/IEC 20000. Information technology - Service management. Geneva, Switzerland: International Organization for Standardization, 2011.
8. ISO/IEC 27000. Information technology – Security techniques. Geneva, Switzerland: International Organization for Standardization, 2011.
9. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
10. JAŠEK, Roman, SZMIT, Anna, SZMIT, Maciej. Usage of Modern Exponential-Smoothing Models in Network Traffic Modelling. In Nostradamus 2013: Prediction, Modeling and Analysis of Complex Systems. Heidelberg : Springer-Verlag Berlin, 2013, s. 435-444. ISSN 2194-5357. ISBN 978-3-319-00541-6.
11. JAŠEK, Roman, KOLAŘÍK, Martin, VÝMOLA, Tomáš. APT Detection System Using Honeypots. In Proceedings of the 14th WSEAS International Conference on Automation & Information (ICAI '13). Montreux : WSEAS Press, 2013, s. 25-29. ISSN 1790-5117. ISBN 978-960-474-316-2.
12. KRBEČEK, Michal, SCHAUER, František, JAŠEK, Roman. Security aspects of remote e-laboratories. International Journal of Online Engineering, 2013, roč. 9, č. 3, s. 34-39. ISSN 1868-1646.
13. Vala, Radek; Malaník, David; Jašek, Roman. Usability of software intrusion-detection system in web applications. In International Joint Conference CISIS ´12-ICEUTE ´12-SOCO ´12. Heidelberg: Springer-Verlag Berlin, 2013, s. 159-166. ISSN 2194-5357. ISBN 978-3-642-33017-9.