Standardization of Information Security Management System: ISO/IEC 27001:2005, ITIL®, CoBIT®

http://dx.doi.org/10.3991/ijes.v1i2.2937

Martina Jakábová, Jana Urdziková and Emília Mironovová
Slovak University of Technology in Bratislava, Trnava, Slovak Republic

***Abstract*—Information is currently the most important asset of modern companies. Its security is therefore very important and becomes the top priority of each company. Unfortunately, there is no simple recipe providing 100 % security of information. A company must apply the best security procedures with the aim to achieve an appropriate level of its information security. This paper presents and compares the most widely used approaches to Information Security Management System – ISO/IEC 27001:2005, BS 7799, ITIL® and CoBIT®. Each standard has its own scope, focus and target audience, which complement each other and play an important role in a company. The company should have an implemented methodological guidance of IT management to ensure a consistent approach to IT management and IT security. In addition to the standards and frameworks, other important players in the standardization of information security are e.g. AIM, BISLA®, CMMI®, ISO/IEC 15504–x, AS8015, etc.**

***Index Terms*—information, security, management, company, cycle, standard, framework, model.**

I. INTRODUCTION

History of Information Security (hereinafter "IS") goes far in the past, beginning about 4000 years ago in the ancient Egypt. Rulers, soldiers, diplomats and businessmen in the following millennia realized the importance of protecting the information, and the field began to develop significantly during the World War II [1]. Development of IS and ICT called for additional security attributes of information: the basic safety requirements (ensuring confidentiality, integrity, availability) were gradually enhanced by the new attributes that are listed in the section of Theoretical background of information security management. The emergence of new IS/ICT challenged new security threats that have been dealt with ad hoc [2, 3, 4]. Since IS begun to play an important role in supporting its activities, companies needed established methodological guidelines in line with governmental guidelines. Several organizations, both private and governmental, have therefore established bodies of standards in order to set up the standards, benchmarks and, in some cases, also IS legislation, so as to maintain an adequate level of security and proper use of funds, and to ensure the adoption of a system of the best security practices. Security procedures have thus become an important tool of achieving the required level of IS. This has been reflected in the activities of standardization bodies, issuing a growing number of standards, methodologies, frameworks etc., and gradually covering all the activities in the areas of IS/ICT governance in a company. Currently, there are several standards, methodologies, frameworks and models, such as ISO/IEC270xx series standards, BS 7799, ITIL®, PRINCE2®, CoBIT®, OPM3®, CMMI®, P–CMM®, PCI DSS etc. [5]. IS is thus becoming an important part of the company security, and a decisive factor in improving company's performance. Actual violation of IS leads to loss of confidence of both business partners and customers [6, 7].

This paper briefly describes and compares selected standards (ISO/IEC 27001:2005, BS 7799) and frameworks (ITIL® and CoBIT®), which are parts of ISMS.

II. THEORETICAL BACKGROUND OF INFORMATION SECURITY MANAGEMENT

IS/ICT significantly influences the development of a company. IS is a prerequisite for the effective performance of a company. In broad terms, this means security of the IS and the protection of the information space and practically the protection of the company's IS/ICT [2].

According to the ISO/IEC 27001:2005 international standard, IS provides information about a wide spectrum of risks, in order to secure continuity of business processes, minimize losses and maximize the return on investment [9, 8, 10]. The European Union and multinational organizations (OECD, OSN, G8, etc.) perceive IS as a world–wide problem. To protect their company's valuable assets and privacy, they establish various institutions and institutional systems (e.g. ENISA, HLIG, etc.), where they set up strategic goals and take measures to meet the goals [11]. IS is of a multilateral character, i.e. it must reflect the interests of the IS/ICT users as well as the rights of personal and legal entities, the data of which are processed in their systems. According to BS 7799 standard, ISMS is a part of the total management system based on the approach to risks, the role of which is to introduce, implement, operate, monitor, revise, maintain and improve the IS [12, 13].

Information is a content of data occurring in various forms: written, oral, image and electronic (digital) forms. It can be processed by various means. Since information is a key asset, its jeopardizing poses a serious problem that should be addressed quickly and efficiently. Existence of a required level of the assets' attributes is a pre–requisite of successful performance of all types of companies [10, 14]. Adequate protection of information is based upon the purpose for which the information is used and what and how it is endangered. The practice frequently encounters combined requirements for protecting information. According to ISO/IEC 27001:2005 and ISO/IEC 27002:2005, basic security requirements for data protection involve confidentiality, integrity, availability, authenticity, accountability and privacy. Confidentiality means ensuring that information is provided and is accessible only to authorized persons. Integrity means ensuring the correctness and completeness of the information in terms of content and form. Availability of information means that the information is accessible to authorized persons whenever they need it – the right information to the right people at the right time. Authenticity of information is to ensure the integrity and originality of a document. Traceability enables to determine which entity conducted safety–related activities, e.g. who entered, changed, deleted or read the information. Finally, protection of data privacy provides protected access to information only to a closer range of authorized users [1, 2, 8, 10, 15].

Nature of IS is best explained in the essence of the OECD guidelines of 2002. The document is binding, but recommendatory in character. It emphasizes the necessity to support the development of security culture, i.e. focus on security in the IS/ICT development and adaptation of new ways of thinking and behaving in the IS/ICT utilization. The guidelines are based on nine basic principles – safety awareness, responsibility, response, ethics, democracy, risk assessment, design and implementation of security, IS management and reassessment. In solving IS and implementing ISMS, it is necessary to consider these principles, which are described in detail in the above–mentioned ISO/IEC 27001:2005 standard. Similar principles are also comprised in a number of policy documents, whether international or national [2, 3, 4].

III. METHODOLOGY OF RESEARCH

Aim of the present paper is, based on the studies and evaluation of the available literature, to analyze and compare selected standards, methodologies, frameworks and models of ISMS (descriptive research). To achieve the aim, we analyzed secondary sources (domestic and foreign professional literary sources, especially standards, methodologies, frameworks and models, studies, documents and journals related to this topic, as well as monographs, handbooks, textbooks, textbooks, websites, etc.) and applied the research methods (the study of literature, literary research, excerpts, their processing and sorting), the methods of obtaining new data (document analysis), methods of the data processing (such as analysis and synthesis, induction and deduction, comparison and generalization). Spreadsheets and word expression interpretation were used as complementary methods.

IV. STANDARDIZATION IN THE FIELD OF INFORMATION SECURITY MANAGEMENT

General support for standardization in the field of IS management initiated a number of norms, standards, methodologies and frameworks. The following sections of the present paper provide a brief overview of the most important standards and frameworks.

A. ISO/IEC 27001:2005

Requirements regarding the implementation on ISMS in a company are provided by the international ISO/IEC 27001:2005 standard, which is owned by ISO and IEC. International Standard of ISO/IEC 27001 published in 2002 was a revised version of BS 7799–2:1999 British Standard (BS 7799–2:2002) [12, 16]. It specifies the basic requirements for design, implementation, operation, monitoring, reviewing and improving the documented ISMS within the company. It describes how to implement security controls adapted to the needs of individual organizations or their parts. It is also used to assess the conformity of internal or external interested parties and certification audits [10, 16, 18, 23]. There is a separate specification for ISMS, fully compatible with the already established quality management systems according to ISO 9001:2008 or environmental management according to ISO 14001:2004 [20]. It complements ISO/IEC 17799:2005 standard. ISO/IEC 17799:2005 is a guidance standard for ISO/IEC 27001:2005; it was therefore renamed as ISO/IEC 27002:2005 in the year 2007 [15]. ISO/IEC 27001:2005 standard can be applied in the companies of all types and sizes, as well as in various business areas [21]. It is designed in a way enabling the company arrange or integrate its ISMS in compliance with the requirements of another management system. The current ISO/IEC 27001:2005 standard is structured into eight chapters and three annexes [18, 23]. The main part of the standard defines mandatory parts of ISMS, especially the area of risk assessment. Annex of the standard describes eleven control areas based on a set of the best practices in the areas of [9, 22, 23, 24]:

1. Security policy.
2. Organization of information security.
3. Assets management.
4. Safety of human resources.
5. Physical security and environmental security.
6. Management of communication and operation management.
7. Management of approaches.
8. Acquisition, development and maintenance of information systems.
9. Managing security of incidents.
10. Managing continuity management of an organization.
11. Compliance with requirements.

References are listed in the conclusion of this paper.

ISO/IEC 27001:2005 is based on a process approach and in compliance with the principles applied in ISO 9001:2008 and OECD Guidelines. Similarly to other ISO standards, ISO/IEC 27001:2005 also comprises a PDCA cycle (Plan–Do–Check–Act) [21, 22]. The goal is to design and operate an IS in compliance with the IS rules, and to update it in case of changes [22].

Slovak Republic adopted the above–mentioned standard under the name of STN EN ISO 27001:2006, which enables effective and clear management of information security in a company. Certificate acquired according to this standard is therefore of international validity: a Slovak company that acquired the ISMS ISO 27001 standard does not need to prove in another country that the requirements of this standard were met.

Introduction of ISMS in a company ensures the protection of assets of any kind (digital information, paper documents and physical assets (computers and networks), knowledge and skills of employees and the protection of natural objects of the organization) [8]. It demonstrates the confidence that the information and the data obtained is handled carefully, the message is defined in terms of safety rules and the risks associated with the threats identified in the process are managed properly. It also declares compliance with the legislative requirements for information security (e.g. Act No. 215/2004 of the Coll. on protection of confident data and on the change and amendments of some laws in the wording of later regulations, Act No. 428/2002 of the Coll. on protection of personal data in the wording of later amendments, Act No. 215/2002 of the Coll. on electronic signature and the change and amendments of some laws in the wording of later regulations, Act No. 618/2003 of the Coll. on copyright and the rights regarding the copyright in the wording of later regulations, Act No. 300/2005 of the Coll., criminal law in the wording of later regulations, Act No. 211/2000 of the Coll. on free access in the wording of later regulations, Commercial Code No. 513/1991 Coll., etc.) [25, 26].

B. BS 7799

The international BS 7799 standard was issued in the year 1995 BSI. The BS 7799:1995 standard was focused on supporting the companies in the ISMS implementation, without emphasizing the performance of risk assessments. Contribution was the achievement of the primary level of information security system and standard security management of security issues in the company [10]. In 1998–1999, the standard was revised and expanded to two parts [10]:

- BS 7799–1:1998 – Code of Practice for Information Security Management. The standard was included into the system of international ISO standards without any substantive changes and it laid the groundwork for the development of ISO/IEC 17799 (published in 2000). It contains a set of security measures and procedures for the management of IS in a company.
- BS 7799–2:1999 – Specification for Information Security Management Systems. After redrafting, the standard was issued in 2002 under the name of BS 7799–2:2002. The aim of the amendment was to harmonize it with the ISO 9001:2008 standard of Quality Management System, ISO 14001 Environmental Management System, and introduction of PDCA cycle. In 2005, BS 7799–2:2002 standard formed the basis of the international ISO/IEC 27001 standards published in 2005. This was to ensure the use of the identical terminology and methods.

BS 7799–3 was issued in 2005 (ISO version of ISO/IEC 27005 – Information Security Management Systems – Guidelines for Information Security Risk Management). The standard is consistent with other ISO/IEC documents, particularly with the aforementioned ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standards. It mainly provides recommendations for the implementation of the requirements set out in ISO/IEC 27001:2005 regarding the risk management and related activities. It is general enough to be used in all companies regardless their size. Recommendations should be accompanied by additional recommendations before they can become the basis for a risk management system in accordance with ISO/IEC 27001:2005. The standard does not declare compliance with the legislative requirements for IS. It is designed for those companies that are involved in ISMS risk management [12].

C. ITIL®

ITIL® (Information Technology Infrastructure Library®) is a complex system of volumes leaving certain freedom in the implementations of processes. It belongs to the portfolio of the best practices of OGC. It is a process – oriented framework for the field of management of IT services [32, 33, 34]. It is suitable for both IT services suppliers and also bigger IT divisions [35]. It is based on the PDCA cycle [32, 33, 34]. ITIL® framework was designed and gradually published since the year 1980 under the name of GITIM, as a response to the demand of the British government with the aim of assuring quality of services and decreasing the IT expenses of the British government and private sector of CCTA. Original framework fastened on the common practice, governmental agencies and private sector. The concepts are similar: providing and supporting IT services. The first set of ITIL®V1 was issued in the year 1989. The whole library contained 46 individual volumes. Continuity between individual volumes was not maintained [33, 34, 36]. In the year 1990, the concept was accepted by the big companies and governmental agencies in Europe. It was gradually introduced to non–governmental institutions and organizations in Great Britain and all over the world. In the year 2000, Microsoft® started using ITIL®V1 as the basis for the development of its own framework entitled Microsoft Operations Framework® (hereinafter “MOF®”).

In the year 2001, ITIL®V1 was revised (denoted as ITIL®V2). ITIL®V2 comprised 10 parts: two basic volumes (Service Support and Service Delivery), which were divided into several brief volumes and other nine volumes [33, 34, 37]. In the year 2006, a new version of the ITIL® glossary was published. In the year 2007, an enhanced version of ITIL®V3 (5 volumes) was published. ITIL®V3 was built upon the control of the IT life–cycle or the control of the value provided by IT to their customers, i.e. consumers of IT services [33, 34, 38, 39, 40]. A new version denoted as ITIL®2011 Edition and issued in 2011comprises five basic volumes – Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement, as well as complementary volumes, such as The Introduction to the ITIL® Service Lifecycle, omitting some processes, adding new processes, check lists of changes and reviewed field of the expertise certification. Amended was particularly the volume of Service Strategy and ITIL® glossary [33, 34, 40, 41]. Framework is neither a standard nor a methodology of ITSM as it does not deal with particular feature of the company’s organizational structure, nor the way of occupying the roles of processes by certain work positions (it gives just recommendations which should/should not be cumulated in one person, and the similarity and contents of both procedures and the project methodology of ITSM implementation [42]. It currently serves as the basis for the development of the process itself. Major advantage of introducing the processes according to ITIL® is the use of agreed terminology (event, incident, problem, activity, role, etc.) facilitating communication between the company with its customers and partners, as well as between individual departments [46].

BSI fastened on ITIL® and defined the standard of BS 15000 – BS 15000–1:2002 IT Service Management – Specification for Service Management, BS 15000–2:2003 IT Service Management – Code of practice for Service Management. In 2005, it was included into the ISO system under the code of ISO/IEC 20000 – ISO/IEC 20000–1:2005 Information Technology – Service Management – Part 1: Specification, ISO/IEC 20000–2:2005 Information Technology – Service Management – Part 2: Code of Practice. Currently, the British standard is replaced by BS ISO/IEC 20000–1:2005 Information Technology – Service Management – Specification, BS ISO/IEC 20000–2:2005 Information Technology – Service Management – Code of Practice [39, 47].

D. CoBIT®

CoBIT® (Control OBjectives for Information and related Technology) is a framework designed in 1996 by the international ISACA for IT governance. It comprises a set of practices enabling to achieve strategic goals of company through the effective utilization of available sources and minimization of IT risks. CoBIT® is primarily designed for managers, auditors and IT users, providing them with a system of processes, indicators and metrics which can be used to introduce the system of IT Governance in order to maximize the benefit of IT utilization. The framework is used to set up or audit information processes in bigger companies [35]. The framework was first time issued in 1996. The second version of 1998 was enhanced by audit procedures, a set of implementation tools, elaborated processes and detailed goals. The third version of 2000 was complemented by managerial procedures within the innovated framework. Major change was that CoBIT® was included into ITGI section. Version 4.0 of 2005 combined several documents into one. Version 4.1 of 2007 (213 p.) classifies IT into four sections representing main chapters of the book, describing 34 processes. There is also PDCA cycle [48]. The final version of CoBIT® is version 5 of 2012, which consolidates and integrates frameworks CoBIT® 4.1, Val IT 2.0 and Risk IT, including ITIL®2011 Edition and relating ISO standards, and comprising the features of BMIS and ITAF models [49]. It defines the IT processes divided into two main fields of process domains – Governance: (Evaluate, Direct and Monitor/EDM) – 5 processes, Management: (Align, Plan and Organize/APO) – 13 processes, (Build, Acquire and Implement/BAI) – 10 processes, (Deliver, Service and Support/DSS) – 6 processes, (Monitor, Evaluate and Assess/MEA) – 3 processes, the structure of which forms a loop representing the life–cycle of the information system. Each of the processes in individual area splits into detail activities, their inputs and outputs. Evaluation scale for all processes has 6 degrees: 0–process does not exist, 5–process is fully optimized. CoBIT®5 is built upon five basic principles [50]:

1. Meeting the needs of each stakeholder.
2. Complete coverage of the company.
3. Roofing of recommendations and standards.
4. Comprehensive approach.
5. Department of governance.

A comprehensive approach provides seven fundamental components [50]:

1. Principles, rules and frameworks.
2. Processes.
3. Organizational structures.
4. Culture, ethics and behavior.
5. Information.
6. Services, infrastructure and applications.
7. People, skills and competencies.

Similarly to ITIL®2011 Edition, CoBIT®5 is based on a fact, that, in order to achieve its goals, the company should identify its business requirements, which will consequently generate the requirements for IT sources, integrated in the IT processes bringing the desired service and information.

E. Other Standards, Frameworks and Models

Besides the above–mentioned standards and frameworks, there are other important players in the field of the IS standardization, e.g. (own source):

1. AIM: A Generic Framework for Information Management (The Amsterdam Model of Information Management).
2. BiSL® (Business Information Services Library®).
3. CMMI® (Capability Maturity Model® Integration).
4. ISO/IEC 15504–x: Software Process Improvement and Capability Determination (well–known as SPICE). Slovak Republic adopted the standard under the name of STN ISO/IEC 15504x:2010: Information technologies. Evaluation of processes.
5. ISO/IEC 38500:2008: Corporate Governance of Information Technology is very similar to AS8015. Slovak Republic adopted the standard under the name of STN ISO/IEC 38500:2011: Corporate governance of information technologies.
6. AS8015 (Australian Standard for Corporate Governance of Information and Communication Technology/ICT.
7. SABSA® (Sherwood Applied Business Security Architecture®).
8. AS/NZS 4360:2004: Risk Management (Australia/New Zealand/Risk management).
9. ISO/IEC 20000x: Information technology. Service Management. Slovak Republic adopted the standard under the code of STN ISO/IEC 20000k:2008 Information technologies – Management of services.
10. TOGAF (Open Group Architecture Framework).
11. Val–IT / Risk–IT – frameworks of investment and risk management.
12. MOF, HPITSM (Hewlett Packard's ITSM Reference Model), PRM–IT (IBM's Process Reference Model for IT) – ITSM frameworks of commercial providers.
13. eTOM (Enhanced Telekom Operations Map) – framework of telecommunication branch.
14. PAS 56 (Publicly Accessible Specification 56).
15. ISO/IEC270xx – Information Technology – Security Techniques – Information Security Management Systems. Slovak Republic adopted the standard under the name of the STN ISO/IEC 270xx standards – Information technologies – Safety techniques.

16. PRINCE2®:2009 (PRojects IN Controlled Environments®).
17. OPM3® (The Organizational Project Management Maturity Model®).
18. P–CMM® (People Capability Maturity Model/People CMM/PCMM/P–CMM/).
19. PCI DSS (Payment Card Industry Data Security Standard), etc.

F. *Comparison of ISO/IEC 27001:2005, ITIL®2011 EDITION and CoBIT®5:2012*

Table I. lists the criteria of IS/ICT ISO/IEC 27001:2005, ITIL®2011 Edition a CobiT®5:2012 in order to compare the currently most widely used approaches toward management and administration.

TABLE I.
COMPARISON OF ISO/IEC 27001:2005 STANDARD WITH ITIL®2011EDITION AND COBIT®5:2012 FRAMEWORKS [ADAPTED BY 5, 8, 13, 56, 57]

STANDARD/ FRAME	ISO/IEC 27001	ITIL®	CoBIT®
CRITERIA			
MEANING	Information Technology – Security Techniques – Information Security management systems – Requirements	Information Technology Infrastructure Library	Control OBjectives for Information and related Technology
TYPE	standard	framework	framework
RECOGNITION	world–wide	world–wide	world–wide
OWNER	ISO IEC	OGC	ISACA
YEAR OF ISSUE	1947	1980	1996
REQUIREMENT	BS 7799–2:2002	governmental organizations from practice	to establish consultation and audit companies
ORIGIN	UK	UK	UK
TARGET GROUP	all in company responsible for security management, IT experts for security management; auditors	providers of IT services, IT experts on all levels of management	top management, IT users, auditors, owners of processes
TYPE OF COMPANY	all companies regardless the type and size	all companies regardless the type and size	big companies with complex infrastructure of IS/ICT
COMMUNITY AND GROUP OF USERS	–	itSMFI (IT Service Management Forum International) ITSMportal (IT Service Management Portal) LinkedIn (group ITIL®)	IT Professional Networking Knowledge Centre
PUBLISHER	ISO	TSO (Stationary Office)	ISACA
ACCREDITATION	BSi group	APMG (APM Group)	ISACA (Information Systems Audit and Control Association)
CERTIFICATION AND QUALIFICATION	link to ISO/IEC 17000:2004 ISO/IEC 27x	ITIL Foundation Level ITIL Intermediate Level ITIL Managing Across the Lifecycle ITIL Expert Level ITIL Master Qualification	Certified Information Systems Auditor (CISA) Certified Information Security Manager (CISM) Certified in the Governance of Enterprise IT (CGEIT) Certified in Risk and Information Systems Control (CRISC) professional education conferences training online education
AREAS OF ACCREDITATION AND QUALIFICATION	link to ISO/IEC 17000:2004	ITIL® framework	IT audit, security, management and risks
TOOLS	–	ITIL® scheme SW templates	list of IT audits and standards, regulations, techniques and tools
LEVEL OF IT MANAGEMENT	tactic, operative	tactic, operative	strategic
ORIENTATION	IS	definition of ICT processes, practical procedures, security management	total management and evaluation of IT
LEVEL OF ORIENTATION	identification and management of IS processes, activities directly connected with IT, security techniques, certification	only direct activities and services of IS/ICT	identification of processes, activities and their aims directly connected with the company IS/ICT
MAPPING FOR THE SECOND DEGREE	possible (processes m:n)	possible (processes m:n)	possible (processes m:n)
INTENSITY OF IMPLEMENTATION	demanding	simple/direct; processes are defined, their implementation is free	difficult due to less understanding clarity; need to design processes; demanding; implementation area; relating with the supply of values (Value Delivery)
STRUCTURE	11 fields 39 aims 133 checks 5000 direct and implied security measures	5 fields 6 operative processes 5 tactic processes 26 processes	2 fields (Governance/ Management) 5 domains (1 – Governance: EDM/ 4 Management: APO/BAI/DSS /MEA) 37 processes 129 aims 265 metrics 210 practices 1115 activities 5 principles 7 components
PUBLICATIONS	1	5	6 CoBIT®5 Product Family
SOURCE	http://www.iso.org/ http://www.sutn.sk/default.aspx	http://www.itil.org/ http://www.itsmfi.org/ http://www.itsm.sk/sk/Home.alej	http://www.isaca.org/
AVAILABILITY	paid form directly in ISO	all volumes are paid in specialized outlets with IT literature	all materials except for regulations for audit are available free to download in electronic form on the website of ISACA group; CoBIT® security; baseline is free in .pdf format

MAJOR ADVANTAGES	provides methodology for implementation of specific assessment of risks in a company and a definition of security aims; protects own assets of company, assures and improves customers' trust; certificate; company image	comes out of practice of proven procedures; applicable also in lower levels of IT management; unified terminology; possible implementation in parts; comprises detailed descriptions, definitions, samples of templates, diagrams, models etc.	designed particularly for strategic IT management of environment and implementation of its audit or quick revelation of the mistakes in its management; enables to set out strategic IT management in compliance with strategic business requirements (IT Governance); involves all aspects of IT management of a company division
MAJOR DISADVANTAGES	does not comprise a list of steps leading to the systems' security in the company	does not cover all aspects of IT management; quite complicated framework	distant from routine informatics; says almost nothing about how to design and implement processes, activities, functions and roles; does not contain basic definitions in the field of process description, provides only a list of inputs, outputs, roles and activities, while giving just their names and a detailed description of what the author thought; implementation of IT systems management is complicated

V. CONCLUSION AND RECOMMENDATION

ISMS standardization plays an important role in the ISMS implementation and management in a company. Each standard, methodology, framework or model has a different focus, complementing each other and thus playing an important role in managing the company. While CoBIT$^{\circledR}$ and ISO/IEC 27001 suggest the company's management what to do, ITIL$^{\circledR}$ tells how to do it from the aspect of IT service management. ISO/IEC 27001 focuses only on IS. It is a tool of IT management, i.e. management of IT departments responsible for operation. On the other hand, CoBIT$^{\circledR}$ is a framework for IT Governance, i.e. in terms of the functioning and role of IT from a position of senior management, which may not have a deep knowledge of IT and no focus on IS. It is designed for those who have responsibility for business processes and technology, those who depend on the relevance and reliability of information processed through IT and also for those who provide services in the field of the IT quality, management and control. CoBIT$^{\circledR}$ has thus a broader scope than ITIL$^{\circledR}$. The fundamental difference between CoBIT$^{\circledR}$ and ITIL$^{\circledR}$ is that CoBIT$^{\circledR}$ has not come out from practice, but it is the work of several professional auditing and consulting companies, which corresponds to the language used in publications. For people with IT experience, CoBIT$^{\circledR}$ processes may seem less clear and legible than the ones defined in ITIL$^{\circledR}$, and implementation therefore may be more demanding for them. However, the advantage of CoBIT$^{\circledR}$ is that its publications are freely available for download on the Internet. CoBIT$^{\circledR}$ is thus based on a number of existing IT practices. It is sometimes referred to as an "integrator" summarizing various IT practices under one roof, while helping link these practices with business requirements. Frameworks and standards are not mutually exclusive, but rather complementary. Processes according to ITIL$^{\circledR}$ and ISO/IEC 27001 are commonly used for tactical and operational management. CoBIT$^{\circledR}$ is used at the highest level of IT management, providing management framework based on a model of IT processes. We can say that ITIL$^{\circledR}$ or ISO/IEC 27001 cover specific areas of IT and can be inserted into the CoBIT$^{\circledR}$ framework. On the level of processes, mapping is in the ratio m:n, i.e. certain set of processes of the CoBIT$^{\circledR}$ framework corresponds to certain set of processes according to ITIL$^{\circledR}$ and ISO/IEC 27001.

It is important that the top management of the company took full responsibility for the IT management to actively manage IT strategy. Company management should assert that the company has implemented a standard, framework or methodology of IT management ensuring a unified approach to IT management and IT security within the company [5, 56, 57].

REFERENCES

[1] M. Královič and D. Olejár, D. (2008). *Štandardizácia v oblasti informačnej bezpečnosti. Standardization in the Field of Information Security*. Diploma Thesis. Bratislava, 2008. Comenius University in Bratislava, Faculty of Mathematics, Physics and Informatics. Department of Informatics, 71 p. [Online]. Available: http://www.dcs.fmph.uniba.sk/diplomovky/obhajene/getfile.php/Diplomovka.pdf?id=205&fid=373&type=application%2Fpdf.

[2] *Národná stratégia pre informačnú bezpečnosť – príloha 2. National Strategy for Information Security – Annex 2*. (2009). [Online]. Available: http://www.google.sk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&ved=0CDAQFjAA&url=http%3A%2F%2Fwww.informatizacia.sk%2Fext_dok-narodna_strategia_pre_ib_priloha_2%2F6170c&ei=4SANUZ0a54rgBODvgMAM&usg=AFQjCNG8VccT4Td0631jj5KhBC042x9NqQ.

[3] *Návrh legislatívneho zámeru zákona o informačnej bezpečnosti.* Draft of Legislative Intention of the Act on Information Security (2009). [Online]. Available: http://www.finance.gov.sk/Default.aspx?CatID=7446.

[4] *Návrh. Legislatívny zámer zákona o informačnej bezpečnosti.* Proposal. Legislative Intention of the Act on Information Security (2010). [Online]. Available: http://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CC8QFjAA&url=http%3A%2F%2Fwww.informatizacia.sk%2Fext_dok-zamer_zakona_o_ib%2F9131c&ei=dYYNUcnMGOeM4gTXgoDgCQ&usg=AFQjCNFV629dsJmZaSm333VS0ZWivlNE7g&sig2=chgtB8xPYtuF9Aa4501Gtg&bvm=bv.41867550,d.Yms.

[5] H. Susanto, N. M. Almunawar and Ch. Y. Tuan. (2011). *Information Security Management System Standards: A Comparative Study of the Big Five.* In: International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05., 113505-6969 IJECS-IJENS, ©October 2011. IJENS. [Online]. Available: http://www.ijens.org/vol_11_i_05/113505-6969-ijecs-ijens.pdf.

[6] TASR. (2006). *Informačná bezpečnosť je významným činiteľom pri zvyšovaní výkonnosti podniku. Information Security is a Significant Agent in the Company Performance Improvement*. [Online]. Available: http://ekonomika.sme.sk/c/3048201/informacna-bezpecnost-je-vyznamnym-cinitelom-pri-zvysovani-vykonnosti-podniku.html.

[7] J. Lipianska and I. Hlavatý. (2011). *Informačná bezpečnosť podniku v kontexte krízového vývoja hospodárstva. Information Security Company in the Context of the Crisis Development of Economy*. [Online]. Available: http://of.euba.sk/zbornik2011/ZBORNIK%20VEDECKYCH%20STATI%202011-PDF/KIOF/LIPIANSKA_J._HLAVAT%C3%9D_I._KIOF.pdf.

[8] M. Šolc. (2011). *Informačná bezpečnosť v spoločnosti. Information Security in Society*. [Online]. Available: http://emi.mvso.cz/EMI/2011-01/04%20Solc/Solc.pdf.

[9] *ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO Standard, 2005.

[10] Ľ. Socha. (2010). *Manažérske systémy integrovaného riadenia. Management systems, integrated management.* Catholic University in Ružomberok. VERBUM, ISBN 978-80-8084-608-4. [Online]. Available: http://web.tuke.sk/lf-kmlp/Ucitelia/Socha%20Lubos/MANAK/Studijny%20material/MSIR.pdf.

[11] J. Danišová and M. Česalová. (2010). *Informačná bezpečnosť. Information Security*. Diploma Thesis. College of Management in Trenčín. Trenčín. [Online]. Available: http://www.cutn.sk/Library/Thesis/2010/Danisova.pdf.

[12] *BS 7799-3:2005 – Information Security Management Systems – Guidelines for Information Security Risk Management*, BS, 2005.

[13] F. Kaluža. (2006). *Manažérsky prístup v riešení informačnej bezpečnosti firmy. Managerial Approach to Information Security Solution of Firm.* In: Information Security. [Online]. Available: http://www.securityrevue.com/article/2006/06/manazersky-pristup-v-rieseni-informacnej-bezpecnosti-firmy/.

[14] B. Stehlíková and P. Horovčák. (2011). *Manažment informačnej bezpečnosti vo verejnej správe v podmienkach miestnych samospráv. Information Security Management in the Public Sector In Conditions of Local Government*. [Online]. Available: http://ekonomikavs.fvs.upjs.sk/pdf/Stehlikova_Horovcak.pdf.

[15] E. Virčíková. (2007). *Integrované manažérske systémy. (Učebné texty pre poslucháčov 2. ročníka Bc. štúdia). Integrated Management Systems. (Textbook for Students of 2nd Year Bc. Study)*. In: ELFA, s.r.o., Košice. Faculty of Metallurgy, Technical University of Košice. ISBN 978–80–8073–761–0. [Online]. Available: http://www.jjj.ic.cz/subory/IMS_skripta.pdf.

[16] *ISO/IEC 27001*. [Online]. Available: http://www.qscert.sk/sluzby/certifikacia-manazerskych-systemov/iso-iec-27001.html?page_id=845.

[17] Ltd., IsecT.iso27001security. [Online]. Available: http://www.iso27001security.com/html/iso27k_toolkit.html.

[18] *ISO/IEC 27001:2005 – Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO, 2005.

[19] *BS 77999-3:2006 – Information Security Management Systems. Guidelines for Information Security Risk Management*, BS, 2006. [Online]. Available: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799-3/$FILE/Obsah_BS7799-3-2006.pdf.

[20] *Certifikácia systémov manažérstva bezpečnosti informácií podľa ISO 27001. Certification of Information Security Management Systems According to ISO 27001*. [Online]. Available: http://www.tuv-sud.com/slovakia/sk/ponukane-sluzby/certifikacia-systemu-manazerstva/iso-27001-certifikacia-systemu-manazerstva-bezpecnosti-informacii.

[21] *Systém manažérstva informačnej bezpečnosti. Information Security Management System*. [Online]. Available: http://www.isoauditor.sk/iso-iec-27001.

[22] P. Manda. (2010). *ISO 27001 – vlastnosti a prínosy. ISO 27001 – Properties and Benefits.* In: eFOCUS 1, 2010. [Online]. Available: http://www.efocus.sk/images/uploads/36a_37.pdf. 36 – 37 p.

[23] *ISO/IEC 27001:2005/ISMS*. [Online]. Available: https://wwws.vhbuild.com/generalinfo/guserinfo-s1.htm.

[24] O. Eckel. *ISO 27001 – Informačná bezpečnosť so systémom. ISO 27001 – Information Security Management System*. [Online]. Available: http://sk.cis-cert.com/System-Certification/Information-Security/ISO-27001/Information-Security-Management-System.aspx.

[25] *Systém manažérstva bezpečnosti informácií ISO/IEC 27001. Information Security Management System ISO/IEC 27001*. (2011). [Online]. Available: http://www.systemyriadenia.sk/24/ISO-27001.xml.

[26] G. Bogdanovská. (2008). *Bezpečnosť informácií – jej dôležitosť a možnosti zabezpečenia. Information Security – Its Importance and Security Options*. [Online] Available: http://katedry.fmmi.vsb.cz/639/qmag/mj57-cz.pdf.

[27] *ISO 27001 Online. ISO 27001 Security*. [Online]. Available: http://www.27001-online.com/.

[28] *ISO27k Infosec Management Standards. ISO 27001 Security*. [Online]. Available: http://iso27001security.com/.

[29] *STN ISO/IEC 27001:2006 – Informačné technológie – Zabezpečovacie techniky – Systémy manažérstva informačnej bezpečnosti – Požiadavky. Information Technology – Security Techniques – Information Security Management Systems – Requirements*, 2006.

[30] *ISO/IEC 27002:2005 – Information Technology – Security Techniques – Code of Practice for Information Security Management*, ISO, 2005.

[31] E. Verheul. (2011). *Practical implementation of ISO 27001/27002. Lecture 2. Security in Organizations*. [Online]. Available: http://www.cs.ru.nl/~klaus/secorg/Slides/02_IS_IMPL_20v0.51.pdf.

[32] *Čo je to ITIL®. What is ITIL®*. [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Co-je-to-ITIL-.alej.

[33] *História ITIL®. History of ITIL®*. (2012). [Online]. Available: http://boom.netlife.sk/2012/07/historia-itil/.

[34] J. Hospes. *ITIL® - Nejrozšířenější přístup k řízení informatiky. ITIL - the Most Widely Used Approach to IT management.* In: IT SYSTEMS 12/2005. (2005). [Online]. Available: http://www.systemonline.cz/clanky/itil-nejrozsirenejsi-pristup-k-rizeni-informatiky.htm.

[35] *Metodiky a normy. Methodologies and Standards.* (2012). [Online]. Available: http://www.perpartes.cz/o_nas/metodiky.

[36] *Charakteristiky ITIL®V1. Characteristics of ITIL®V1*. (2013). [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Rozdiely-medzi-verziami-ITIL-/Charakteristiky-ITIL-V1.alej.

[37] *Charakteristiky ITIL®V2. Characteristics of ITIL®V2*. (2013). [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Rozdiely-medzi-verziami-ITIL-/Charakteristiky-ITIL-V2.alej.

[38] *Charakteristiky ITIL®V3. Characteristics of ITIL®V3*. (2013). [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Rozdiely-medzi-verziami-ITIL-/Charakteristiky-ITIL-V3.alej.

[39] *História a vývoj ITIL®. History and Development of ITIL®*. (2013). [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Historia-a-vyvoj-ITIL-.alej.

[40] *Zmeny v ITIL®2011 Edition. Changes in ITIL®2011 Edition*. (2013). [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Rozdiely-medzi-verziami-ITIL-/Zmeny-v-ITIL-2011-Edition.alej.

[41] *Procesné riadenie IT. IT Process Management.* (2012). [Online]. Available: http://www.dcit-consulting.sk/sk/konzultacie/procesne-riadenie-IT.

[42] M. Medvecký. (2011). *Manažment IT služieb, ITSM a ITIL. Prednášky. IT Service Management, ITSM and ITIL. Lectures*. [Online]. Available: http://files.gamepub.sk/RTS/predn%C3%A1%C5%A1ky/RTS-8%20ITIL%20a%20ITSM%20%282011%29.pdf.

[43] J. Krausko, M. Pecho and I. Polický. (2008). *Prípadová štúdia zavedenia manažmentu IT služieb. A Case Study of the Implementation of IT Service Management*. Diploma Thesis. Slovak University of Technology in Bratislava. Faculty of Informatics and Information Technologies. 124 p. [Online]. Available: http://diplomovka.sme.sk/zdroj/3464.pdf.

[44] Bon van J. (2012). *ITIL® Pocket Guide 2011 Edition. Best Practice. Van Haren Publishing. Zaltbommel.* 1st Edition, 2012. ISBN 978-90-87-53-676-2. [Online]. Available: http://www.exin-library.com/Samplefiles/9789087536763SMPL.pdf.

[45] *ITIL®Training Zone*. (2011). ITIL®2011 Mind Maps. [Online]. Available: http://martinliu.cn/wp-content/uploads/downloads/2012/01/ITIL_2011_Mind_Maps.pdf.

[46] J. Doboš. (2012). *Riadenie telekomunikačných systémov. Zadanie č. 2. Management of Telecommunications Systems. No. 2.* Slovak University of Technology in Bratislava. Faculty of Electrical Engineering and Computer Science. Institute of Telecommunications. [Online]. Available: http://shaolinsala.wz.cz/Rtszadanie2-Dobos.pdf.

[47] J. Skála. (2006). *Od BS 15000 k ISO/IEC 20000. From BS 15000 to ISO/IEC 20000.* [Online]. Available: http://si.vse.cz/archive/proceedings/2006/od-bs-15000-k-iso-20000.pdf.

[48] *COBIT® tajemství zbavený. COBIT Stripped of Mystery*. (2010). [Online]. Available: http://www.cleverandsmart.cz/cobit-tajemstvi-zbaveny/.

[49] *Predstavujeme COBIT®5. COBIT®5 Introduction.* (2013). [Online]. Available: http://www.optit.sk/index.php/83-all/novinky/91-predstavujeme-cobit-5.

[50] *COBIT®5*. (2013). [Online]. Available: http://www.ict-123.com/Procesn%C3%AD%C5%99%C3%ADzen%C3%AD/Metody/COBIT5.aspx.

[51] ISACA. Newsletter, číslo 2/2012. [Online]. Available: http://www.isaca.sk/domain/isaca/files/newsletter/newsletter-2-2012-verzia-2.pdf.

[52] R. Stroud. (2012). *5 Essential Facts about COBIT®5. Webinar.* [Online]. Available: http://www.isaca.org/COBIT/Documents/5-Essential-Facts-about-COBIT.pdf.

[53] R. Stroud. (2012). COBIT®. Simplixy Complex Standards. [Online]. Available: http://www.isaca-km.org/events/materials/2012-05_grc_symposium_session2.pdf

[54] ISACA (2012). *COBIT®5 Introduction*. [Online]. Available: http://www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf.

[55] ISACA (2012). *COBIT®5 Introduction*. [Online]. Available: http://www.misrc.umn.edu/seminars/slides/2012/An-Introduction%20COBIT%205%2018%20May%202012%20UM.pdf.

[56] *Vzťah ITIL® a CobiT®. Relationship between ITIL® and CobiT®.* (2013). [Online]. Available: http://www.itsm.sk/sk/-ITSM-ITIL/Vztah-ITIL-a-dalsich-pristupov/Vztah-ITIL-a-CobiT.alej.

[57] R. Sheikhpour and N. Modiri. (2012). *An Approach to Map COBIT Processes to ISO/IEC 2700. Information Security Management Controls*. In: International Journal of Security and Its Applications, Vol. 6, No. 2, April. [Online]. Available: http://www.academia.edu/1587532/An_Approach_to_Map_COBIT_Processes_to_ISO_IEC_27001_Information_Security_Management_Controls.

[58] J. Šalgovičová, J. Urdziková and V. Prajová, "Research of the Factors that Influence the Selection and Implementation of Integrated Marketing Communication Tools in Respect", in: Fórum Manažéra. Managers Forum. - ISSN 1336-7773. - Č. 1, 42-45 p. 2012.

[59] A. Saniuk, S. Saniuk and K. Witkowski (2011). *Using Activity Based Costing in the Metal Working Processes.* In: METAL 2011. Conference proceedings. [Online]. Available: http://www.metal2013.com/files/proceedings/metal_11/lists/papers/1088.pdf.

[60] M. Relich, "CP-based decision support for scheduling", in: Applied Computer Science, vol. 7, no. 1, pp. 7-17. 2011.

[61] M. Horová and P. Taušl Procházková, "*Podnikatelská kultura, image podnikatele a jejich řízení. Entrepreneurial Culture, the Image of Entrepreneurs and their Management*". University of West Bohemia in Pilsen, Pilsen, 128 s. ISBN: 978-80-261-0012-6, 2011.

[62] J. Urdziková [head of research team], M. Jakábová, [member of research team], P. Večeřa[member of research team], Bezpečnosť informačných aktív ako integrálna súčasť systému manažérstva kvality v súlade s princípmi spoločensky zodpovedného podnikania (akronym: SelnA): Záverečná správa k projektu v rámci Programu na podporu mladých výskumníkov (č. 6533). Security of Information Assets as an Integral Part of the Quality Management System in Accordance with the Principles of Corporate Social Responsibility (acronym: SeInA): The Final Report within the framework of the support for young researchers (č. 6533). - Trnava: STU in Bratislava MTF UPMK, 2013. - 24 p. + Appendix, 2013.

[63] J. Urdziková and M. Jakábová, Štúdia - analýza súčasného stavu systému bezpečnosti informačných aktív v organizáciách na Slovensku. Výsledky, zistenia a závery projektu SeInA (č. 6533) v rámci Programu na podporu mladých výskumníkov. The Study - an Analysis of the Current State of Security of Information Assets in Organizations in Slovakia. The results, findings and conclusions of the SeInA project (No. 6533) within the framework of the support for young researchers (č. 6533). Appendix E. - Trnava: STU in Bratislava MTF UPMK, 2013. -38 p., 2013.

[64] M. Jakábová and J. Urdziková, "Štandardizácia systému manažérstva informačnej bezpečnosti", in: Informačné a komunikačné technológie v riadení a vzdelávaní [elektronický dokument] : Medzinárodný vedecký seminár. 1.3.2013 Nitra, SR. - Nitra : Slovenská poľnohospodárska univerzita v Nitre, 2013. - ISBN 978-80-552-0983-8, 2013.

AUTHORS

Martina Jakábová, MSc. Eng., PhD. is a senior assistant and vice-director for entrepreneurial activity, lifelong education and public relations in the Slovak University of Technology in Bratislava, Faculty of Materials Science and Technology in Trnava, Institute of Industrial Engineering, Management and Quality, Paulínska 16, 917 24 Trnava, Slovakia. She has expertise in the field of project and process management and information technologies. She has dealt with analysis, implementation, optimization of the projects and processes in organizations, while actively participating in the projects (martina.jakabova@stuba.sk).

Jana Urdziková, MSc. Eng., PhD. is a senior assistant in the relations in the Slovak University of Technology in Bratislava, Faculty of Materials Science and Technology in Trnava, Institute of Industrial Engineering, Management and Quality, Paulínska 16, 917 24 Trnava, Slovakia. Her teaching and research activities are focused on the field of quality management, process management, management of claims, statistic methods of quality control and monitoring customer satisfaction. She has participated in the research projects (jana.urdzikova@stuba.sk).

Emília Mironovová, PhDr. is a lecturer and head of language training in the Slovak University of Technology in Bratislava, Faculty of Materials Science and Technology in Trnava, Department of Humanities and Social Sciences, Paulínska 16, 917 24 Trnava, Slovakia (emilia.mironovova@stuba.sk).

The submitted paper is an outcome of the research and data collection for the project entitled "Security of Information Assets as an Integral Part of the Quality Management System in Accordance with the Principles of Corporate Social Responsibility" (acronym: SeInA). The project was prepared within the framework of the support for young researchers at the Slovak University of Technology in Bratislava. It fastens on and enhances the partial objectives of the VEGA project No. 1/0558/12 entitled "Research of the Factors Influencing the Selection and Implementation of Integrated Marketing Communication Tools with Regard to Information Security and Consumer Protection", which is currently being dealt with at the Faculty of Materials Science and Technology in Trnava.

Submitted, June, 21, 2013. Published as resubmitted by the authors on June, 30, 2013.