FRAMEWORKS FOR AUDIT OF AN INFORMATION SYSTEM IN PRACTICE

Dalibor Drljača
Europrojekt centar, drljacad@gmail.com

Branko Latinović
Panevropski univerzitet APEIRON, branko.b.latinovic@apeiron-edu.eu

General survay
DOI: **10.7251/JIT1602078D** UDC: **007:004.65]:005.334**

Abstract: The IT function became the backbone of the company and the central driving force of the entire operations of an organization. Modern electronic commerce is very dependent on the quality of information system supported with information technology. Safety aspects of business and electronic transactions transfer (Internet-supported), particularly in the banking sector, require a more complex audit of the organization, both financial and the information system audit. This paper presents the basic and in practice most frequently applied standards and guidelines for checking of security controls in information systems. The work presents the COBIT and ITIL as the two most prevalent methodologies for quality audit of information systems with the presentation of two ISO 27000 series of standards on information security.

Keywords: audit frameworks, IT audit, IT Governance, COBIT, ITIL, ISO27000.

INTRODUCTION

Modern business strongly depends on information technologies (IT) and other relevant auxiliary technologies. The supporting information system (IT supported or not) must be properly established. Weak or bad established information system with corresponding infrastructure not aligned with strategic goals and needs of business ultimately lead to additional and usually not necessary extra costs for the company.

Therefore, information system management must be considered as a very important business process. Proper information management, timely and adequate use of information are providing necessary market advantage, and therefore IT governance and IT auditing are becoming leading concepts today. These concepts are implemented very often in large and complex organisations in order to have overall insight over organisation's activities and for trend analyses.

Linking management and IT is a key for the success of business. Some of the leading problems for already established information systems are a timely collection of information, processing in most efficient manner, but also storing and keeping it out of sight of competitors. To evaluate the quality of the information system in use and its functionality, it is necessary to implement the process of information system auditing. By its nature, this audit process is very demanding and complex. It is even more complex than a classic financial audit. Today, there are a number of standards and frameworks for this kind of audit. Most known and popular are COBIT, ITIL, set of ISO standards, COSO, VAL IT etc. This paper gives an overview of these most important and used

frameworks for information system audit process enabling quality IT management.

IT Governance and Auditing

Van Grembergen defines IT governance as „*the organisational capacity exercised by the Board, Executive Management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT*"[22]

Gartner Inc. consulting company also provided definition that defines IT governance as "*the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals*" [6]

IT governance includes following areas [14]:
- *Strategic alignment*;
- *Value delivery*;
- *Resource management*;
- *Risk management*; and
- *Performance measurements*.

Strategic alignment ensures adequate linking of business and IT strategies and plans. They define, maintain and confirm or support IT organisational values and also define and manage IT business operations in line with regular business activities.

Value delivery enables IT to provide promised and projected advantages realizing strategies and concentrating on costs optimisation and IT investments.

Resource management aims at optimal investments and adequate governance of critical IT processes, such as applications, information, infrastructure and human resources. Key issues relate to the optimisation of knowledge and infrastructure.

Risk management must be implemented and realized at all levels in the organisation – from employees up to the top level management – in order to achieve risk transparency and their mitigation with a clear definition of measures for risk management responsibility.

Performance measurement is needed in order to follow and monitor implementation of strategies and projects, use of resources, working processes and provision of services using „*balanced scorecard*"[16] (measuring and comparing selected indicators) that is used to follow the success of actions and meeting strategy goals along the classical accounting measurement methods. From previous explanation it is obvious that it is necessary to invest a lot of efforts, time and resources to establish a quality information system that will serve a purpose. However, it is not enough to establish the system, but to maintain it is even more important.

Auditing of information systems is relatively new discipline (appearing from the 1960s) intending to become a multidiscipline scientific field that links organisational, strategic and IT aspects of company's business. Historically, auditing of information systems appears as a need for an extension of standard and traditional financial audit in the moment when auditors' limited knowledge of IT requested additional IT knowledge or externally engaged IT professionals. However, there is a significant difference between two types of auditing. The role of the financial audit is **to evaluate if the organisation is complying with standard accounting practices**. From the other hand, the aim of the information system auditing is **to evaluate design and effectiveness of the system using organisation's internal controls**. Therefore, it is not possible to equalize this auditing with the internal auditing.

The definition of information system auditing states that it a process of collecting and evaluating claims on how information system **preserves properties of the company, data integrity and enables more effective and more efficient use of resources for the achievement of business goals** [3].

From the definition, it is obvious that the object of audit is systematic, quality and careful review of controls within all parts of information systems. From this, we can draw basic auditing tasks [18]:
- To evaluate and estimate present status of the system (maturity, level of success),
- To discover risk areas and level of risk, and
- To provide recommendations to the management on practice for the improvement of the governance.

The information system auditor must have broad knowledge and experience not only of business and local legislation, but he/she must also have a broad knowledge of information and communication technologies and modern trends in the field in order to evaluate properly the possible risks.

Given that this is a very complex area and that it requires a holistic approach to problem solving, the practice shows a number of standards and frameworks for auditing of information systems.

INFORMATION SYSTEM AUDITING FRAMEWORKS

Frameworks of information system auditing represent guidelines for the auditor's work and the model of implementation of the audit process for systematic (qualitative and quantitative) collecting and processing data required for the preparation of the audit findings. As there are different schools and approaches to the study of certain areas, it is clear that the frameworks for revision occur in multiple forms. In this paper, we will mention only three most important - COBIT, ITIL, and ISO related standards.

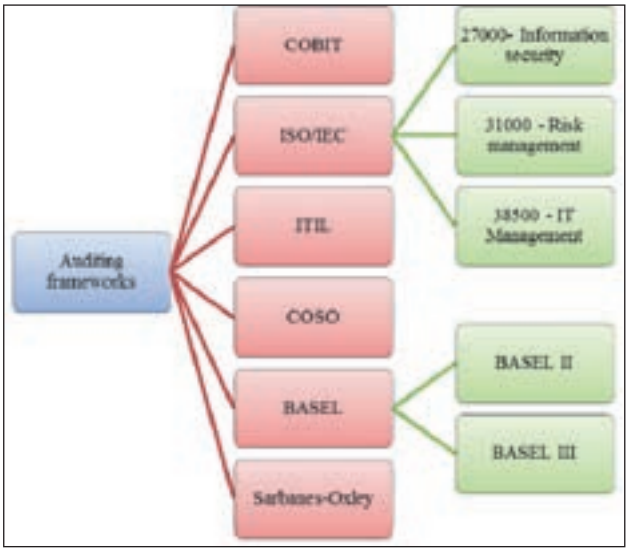

Figure 1. Most used auditing frameworks (author)

COBIT

COBIT (*Control Objectives for Information and Related Technologies*) is a framework made by ISACA (*Information Systems Audit and Control Association, http://www.isaca.org*) and ITGI (*IT Governance Institute, http://www.isaca.org/itgi/Pages/default.aspx*) with the aim to assist management of information technologies (systems). It represents one of the most popular frameworks for information system control, published for the first time in 1996, while actual version 5 was published in 2012. [8]

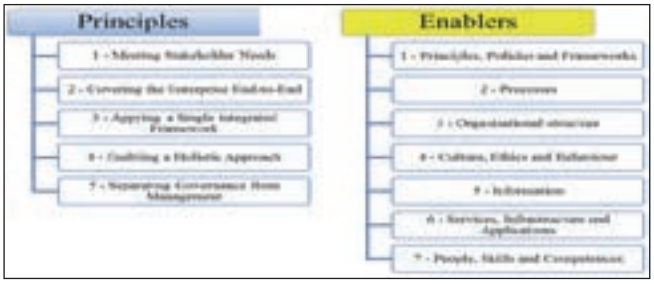

Figure 2. COBIT 5 principles and enablers (author)

COBIT5 *principles and enablers* are generalized and therefore applicable to all companies, regardless of size, types, and ownership. As such, COBIT5 recognizes 7 enablers, which in principle represent factors that individually or collectively influence organisational IT governance and management.

Also, COBIT5 contains 34 control objectives and 37 processes, the fulfilment of which allows the successful achievement of the objectives of functional information systems. These are grouped into five domains [9]:

- *Evaluate, Direct and Monitor* – EDM,
- *Align, Plan and Organise* – APO,
- *Deliver, Service and Support* – DSS,
- *Monitor, Evaluate and Assess* – MEA,
- *Build, Acquire and Implement* – BAI.

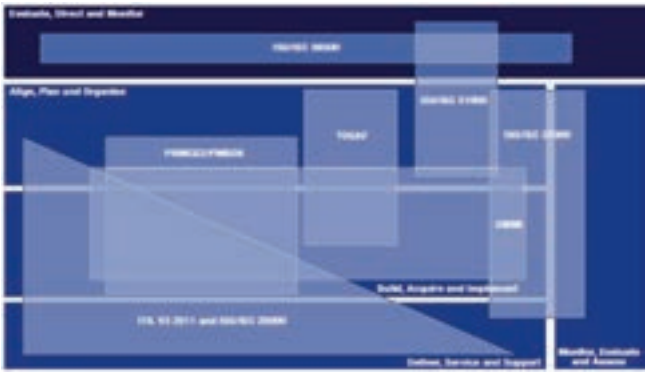

Figure 3. COBIT 5 covers issues from most of frameworks and standards (taken from [9] pg.61.)

As a standard, COBIT5 is useful for different types of users [13]:

- For **managers** – to assist understanding of the information system, to assist decision making on level of safety and control, to provide a basis for investment decisions, to increase efficiency in decision making, to assist in governance and definition of the strategic plan for the information system, to assist in improvement of IT architecture and purchase of necessary ICT technologies, to assist in follow-up and monitoring of system performance, etc.
- For **end-users/employees** – to assist understanding of the information system, to assist understanding of safety and control levels, to assist understanding of organisational strategies etc.
- For **auditors** – to assist understanding of the information system, to assist understanding of safety and control levels, to assist understanding of organisational strategies, to assist in identification of the IT controls and its infrastructure, to help traceability of information in the system, etc.

ITIL

ITIL (*IT Infrastructure Library*) presents a set of best practices for IT service management, both in the introduction and in the improvement. In its essence, ITIL advocates the need to harmonize IT services with needs of business and supports its core processes by providing guidance to the organization and individuals for the use of IT tools to facilitate business change, transformation and growth [2]. The author of ITIL methodology is British *Central Computer and Telecommunications Agency* (*CCTA*) that was reorganised from 2000 as *UK Office of Government Commerce* (*OGC*). They created ITIL by the end of 1980s as a set of guidelines for the use of IT services. As such, it was an obligation for all institutions and bodies of the UK public administration. GITIM (*Government Information Technology Infrastructure Management*) was the first official version of ITIL, while the second version was published in 2001, and actual version 3 was introduced in 2007. The latest, third version, adopts the paradigm of management of IT services' life cycle with strong emphasis on business integration of IT [15]. The AXELOS company (https://www.axelos.com) took over ITIL in July 2013 as a joint venture of CAPITA (http://www.capita.co.uk) and the *Cabinet Office of British Government* (http://www.gov.uk/cabinetoffice), with further authorities over licencing of use of ITIL's intellectual property rights [23].

ITIL as process and business-oriented, uses so-called *top-down approach*. The basis of ITIL consists of five main (5) processes described in 5 volumes of ITIL [1] [19]:

- ***ITIL Service Strategy*** - used for defining of strategic elements as initial phase of IT services lifecycle (who are consumers, what are their needs, which resources are needed for development etc.);
- ***ITIL Service Design*** - used to ensure effective design of new or improved services meeting customer needs, with the development of mechanisms for monitoring and evaluation of effectiveness and efficiency of processes;
- ***ITIL Service Transition*** - used to enable evaluation and testing of design from the previous phase and for transition from the service model to provision of service;
- ***ITIL Service Operation*** – used for provision of services including daily status monitoring, managing daily routines and users demands, etc.; and
- ***ITIL Continual Service Improvement*** – used to exploit measuring mechanisms and for improvement of the level of provided services, technologies, as well as for efficiency and effectiveness of the global system for services' management.

Figure 4. Integration across the service lifecycle (from [4] pg.9.)

There are at least three factors influencing success and acceptance of ITIL. The first one is that ITIL methodology is broadly available to all and that it is maintained by the governmental non-profit organisation. Second, ITIL is accepted by the largest global

organizations and the third factor is the existence of a large number of learning materials (websites and books) for achievements of ITIL goals [7].

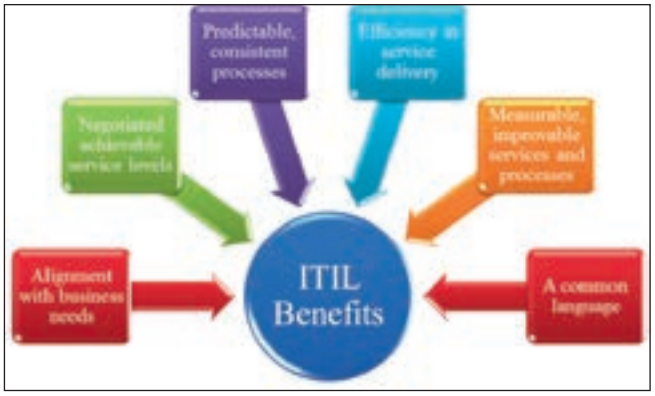

Figure 5. Benefits of implementing ITIL (adapted from [1])

ISO 27000 family of standards

The family of ISO/IEC 27000 standards deals mainly with setting up of a valid system for management with information security called *Information Security Management System* – ISMS. The definition and vocabulary of ISMS were given in ISO/IEC 27000:2014 (third version). More details on ISO/IEC 27000 family of standards are given in Table 1.

The standard ISO/IEC 27001:2013 provides precise requirements for setting up, implementation, maintenance and continuous improvement of ISMS within the organizational context. It also incorporates requirements for evaluation and treatment of information security risks, tailored in accordance with the need of the organisation. The requests are more generic in order to be implemented in all organizations regardless of its type, size or nature. Conceptually, the standard is composed of seven chapters, as follows [11]:

1. Context of the organisation;
2. Leadership;
3. Planning;
4. Support;
5. Operation;
6. Performance evaluation;
7. Improvement; and
8. Annex A with a list of controls and their objectives.

Standard ISO/IEC 27002 started as ISO/IEC 17799 in 2000 and in 2005 was renamed and renumbered into ISO/IEC 27002. It presents a codex for information security practices and is created for the use in organizations as a reference for selection of controls in process of ISMS implementation based on ISO/IEC 27001, or as guidelines for implementation of wide accepted controls related to the information security. Thus, ISO/IEC 27002 and ISO 27001 standards together are giving recommenda-

Table 1. The family of ISO/IEC 27000 standards (from[10])

ISO/IEC 27000	*Information security management systems — Overview and vocabulary*
ISO/IEC 27001	*Information security management systems — Requirements*
ISO/IEC 27002	*Code of practice for information security controls*
ISO/IEC 27003	*Information security management system implementation guidance*
ISO/IEC 27004	*Information security management — Measurement*
ISO/IEC 27005	*Information security risk management*
ISO/IEC 27006	*Requirements for bodies providing audit and certification of information security management systems*
ISO/IEC 27007	*Guidelines for information security management systems auditing*
ISO/IEC TR 27008	*Guidelines for auditors on information security controls*
ISO/IEC 27010	*Information security management for inter-sector and inter-organizational communications*
ISO/IEC 27011	*Information security management guidelines for telecommunications organizations based on* **ISO/IEC 27002**
ISO/IEC 27013	*Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
ISO/IEC 27014	*Governance of information security*
ISO/IEC TR 27015	*Information security management guidelines for financial services*
ISO/IEC TR 27016	*Information security management — Organizational economics*

tions or list of all controls needed for implementation of ISMS with the aim to decrease a level of risks dealing with security. These standards are very popular and widely used, while their implementation can contribute achievement of main objectives of internal controls of an information system (security aims, IT objectives, and business continuity). ISO/IEC 27002:2013 standard consists of 14 main chapters, as follows [12]:

1. Information security policies;
2. Organization of information security;
3. Human resource security;
4. Asset management;
5. Access control;
6. Cryptography;
7. Physical and environmental security;
8. Operation security;
9. Communication security;
10. System acquisition, development, and maintenance;
11. Supplier relationships;
12. Information security incident management;
13. Information security aspects of business continuity management; and
14. Compliance.

COSO

During 1985, accounting and financial associations in the USA gathered in an alliance named *Committee of Sponsoring Organizations of the Treadway Commission* – COSO (http://www.coso.org) with the main aim to finance public-private initiatives given by the *National Commission on Fraudulent Financial Reporting* [5].

COSO framework states that the internal control is composed of five interconnected elements, and for IT auditing purposes the most important is the fourth one [17]:

1. **Control environment** – senior management must set up a positive environment for control and lead employees with own example to respect and to perform their duties as best as they can;
2. **Risk assessment** – a strategy that supports mission and key objectives of the company must be adopted and it will decrease eventual risks of implementation;
3. **Control activities** –in order to ensure proper functionality of internal controlling system, it is necessary to establish adequate controls that will be regularly monitored;
4. **Information and Communication** – all relevant information must be accessible to employees and to the public in order to have good and successful two-way communication system; and
5. **Monitoring activities** – refers to regular evaluation and monitoring of risks and controls, and if necessary to make improvements and corrections.

Other recommendations and standards

There is a significant number of other guidelines, recommendations, and standards which can be adequately combined with previous ones and with the aim to ensure better use of IT and information systems in daily business.

For example, for the banking sector, there are very important and widely accepted recommendations - **Basel II** (2004) and **Basel III** (2011) - sets of reform measures that are covering banks' information system control [20]. These recommendations underline the importance of information system safety in providing services to customers.

***Sarbanes-Oxley* law** was created in 2002 as an initiative of two (same named) USA congressmen as the response to corporative fraud in the financial reporting. The articles of this law became an obligation for all companies present at any stock exchange in the USA. The aim of the law was to introduce a more efficient system of internal controls over the financial reporting process. This law prescribes that the executive managers are responsible for the implementation of the internal control system in operations enabling management to understand the flow of transactions, including their IT aspects, and with sufficient details in order to identify eventual points of fraud and misuse [21].

Conclusion

Modern business is not possible without computer-supported information systems and relevant tech-

nologies. These can provide a market advantage to the organization, if used properly. A significant question is on the adequacy of these systems and technologies as well as their security issues. Therefore, the auditing of an information system is becoming an unavoidable factor for modern business and organizations. This is even more important considering the fact that IT functions of the company are recognized as a central driver of the organisation, especially in electronic commerce.

IT auditors require special skills and a lot of IT knowledge needed for quality and safety aspects of information system auditing. Such complex educational qualifications require experienced professionals and these professionals are becoming high demand at the labour market. Moreover, the IT professionals are the one most profiting from the present accelerated development of IT and information system auditing.

The aim of this paper was to provide an overview of basic standards and guidelines for information system auditing that are broadly accepted worldwide. A number of standards were intentionally left unexplained (due to the limited space for the paper) such as ISO/IEC 38500, ISO/IES 50000, VAL-IT etc. However, their importance is significant for overall auditing process of information systems and they should be also taken into consideration when planning such venture.

BIOGRAPHY

Dalibor Drljača is a Ph.D. candidate at the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka and has MA in information technology and MA in technologies for the Development of European Projects. His main research interests are in e-Government, audit of information systems and e-Commerce. He is part-time engaged as a Senior teaching and research assistant at Pan-European University APEIRON Banja Luka.

Branko Latinović, Ph.D., is a full-time professor and Dean of the Faculty of Information Technologies at the Pan-European University APEIRON Banja Luka since its establishment. His research interests are in information systems, e-Commerce and e-Government.

REFERENCE

[1] Arraj V(2013) ITIL®: The basics (White paper), The APM Group and The Stationery Office

[2] Axelos What is ITIL® Best practices? https://www.axelos.com/best-practice-solutions/itil/what-is-itil (accessed on 1.8.2016.)

[3] Cangemi MP(2000) Managing the Audit Function: A Corporate Audit Department Procedures Guide 3rd ed., John Wiley & Sons, New York, USA, pg.23.

[4] Cartlidge AS et al. (2012) An Introductory Overview of ITIL v3, itSMF Ltd, UK

[5] COSO About us, http://www.coso.org/aboutus.htm, (accessed on 2.8.2016.)

[6] Gartner Inc. IT Glossary, http://www.gartner.com/it-glossary/it-governance/ (accessed on 14.8.2016.)

[7] Infotrend Poslovni IT certifikati, http://www.infotrend.hr/clanak/2012/2/poslovni-it-certifikati,187,894.html (accessed on 14.8.2016.)

[8] ISACA COBIT 20th Anniversary, http://www.isaca.org/COBIT/Pages/COBIT-20th-Anniversary.aspx#years (accessed on 5.8.2016.)

[9] ISACA (2012) COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT, Rolling Meadows, IL, USA

[10] ISO/IEC (2014) International standard ISO/IEC 27000:2014 (3rd edition), International Organization for Standardization

[11] ISO/IEC (2013) International standard ISO/IEC 27001:2013 (2nd edition), International Organization for Standardization

[12] ISO/IEC (2013) International standard ISO/IEC 27002:2013 (2nd edition), International Organization for Standardization

[13] IT revizija.ba COBIT, http://itrevizija.ba/2011/11/cobit/ (accessed on 3.8.2016.)

[14] IT revizija.ba Upravljanje IT (IT Governance), http://itrevizija.ba/2010/08/upravljanje-it-it-governance/ (accessed on 4.8.2016.)

[15] ITIL Central History of ITIL, http://itsm.fwtk.org/History.htm (accessed on 1.8.2016.)

[16] Kaplan RS, Norton DP (1996) The Balanced Scorecard: Translating Strategy Into Action, Harvard University Press, USA

[17] Monte Negro Ministry of Finance (2011) Priručnik za finansijsko upravljanje i kontrole, Podgorica (available at www.mf.gov.me/pretraga/107135/Prirucnik-za-finansijsko-upravljanje-i-kontrole.html, accessed on 2.8.2016.)

[18] Spremić M. Primjena IT u financijskom izvještavanju Računovodstveni informacijski sustavi (available at http://itrevizija.ba/wp-content/materijal/prezentacije/EFSA_Master_Primjena_IT_u_financijskom_izvjestavanju.ppt and accessed on 4.8.2016.)

[19] The Art of Service Pty Ltd (2009) ITIL V3 Foundation Complete Certification Kit: 2009 Edition Study Guide, Brisbane, Australia

[20] The Bank for International Settlements, Basel III: international regulatory framework for banks, http://www.bis.org/bcbs/basel3.htm (accessed on 14.8.2016.)

[21] U.S. Securities and Exchange Commission (2009) Study of the Sarbanes-Oxley Act of 2002 Section 404 Internal Control over Financial Reporting Requirements, Office of Economic Analysis, USA

[22] Van Grembergen W (2002) Introduction to the minitrack IT Governance and its Mechanisms, Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS)

[23] Wikipedia ITIL https://en.wikipedia.org/wiki/ITIL (accessed on 1.8.2016.)

Submitted: September 24, 2016.
Accepted: December 7, 2016.