Characteristics of Information Security Implementation Methods

Sándor Dombora

Óbuda Univerity, Kandó Kálmán Faculty of Electrical Engineering, Institute of Communication Engineering
dombora.sandor@kvk.uni-obuda.hu

Abstract: However information security is supported by national and international recommendations, standards and laws, their implementation fail to deliver the expected results in several cases. In our fast changing world information plays a central role in the operation of organisations. Implementation of information security it is a must for organisations in order to maintain and improve their competitiveness. Companies are working to attain information security by implementing the requirements of ISO/IEC 27001 standard. Governmental institutes follow the instructions of implementing regulations of the legislation in place. The failure of organisations in attaining information security may have several reasons. Our research in this topic reveals that several times the Information Security Management System (ISMS) implemented does not fit the operation of the organisation, its regulations are not applied or simply are not brought into force. There are several ways to implement information security. The most commonly adopted way of implementation is the development of an ISMS and building information security measures around it. Some organisations develop integrated management systems, others implement information security measures in their organisational processes. Applied methods have impact on the effectiveness of implemented information security systems. This study uncovers the most common deficiencies of ISMS. Analyses and compares the most commonly adopted implementation methods based on the acquired professional experience and scientific literature considered relevant by the author. Comparative analysis, uncovers the strengths and weaknesses of applicability and risk of these implementation methods in different operating environments. As a result organisations may use the outcomes in selecting implementation methods to attain information security and handle their risks successfully.

Keywords: information security, method, comparative analysis

1 Introduction

Nowadays most of the organisations depend on information processing services. These services can be delivered by the organisations themselves, partners or service providers. Sometimes organisations outsource some of their business as well as management and operation processes. In this environment employees and partners process information in order to efficiently and effectively execute processes, improve and maintain the competitiveness of their organisation.

According to the international standard ISO/IEC 27001, information security means confidentiality, integrity and availability [1, 2]. The fact that we mention information security, means that this is not only a technological question. During its implementation all possible occurrences of information available in the organisation should be considered. Complex information protection measures should be placed in operations which support activities of organisation processes executed by employees and partners to enforce security, independently of whether they are supported or not by information systems. Security measures according to the threat types can be classified into physical, logical, organisational and life-cycle related categories.

Organisations depending on their sector and development level apply different types of information technology. The threats affecting the data stored and processed by information systems, depend on the applied technology. Security measures applied to protect information systems should align to their implemented infrastructure.

However, today the business data and information is stored and processed in information systems, printed and spoken versions may occur as well. According to this, there are significant information security threats beyond those, related to the information systems, so information should be protected not only in the information systems, but in every occurrence.

The most significant platform independent information security threat is the so called social engineering, which exploits the ignorance, gullibility and helpfulness of the users. Several research papers pay attention to the fact that the user is the weakest point in the protection of information assets. Amongst others [3, 4, 5] Jeimy J. Cano a The Challenge of Transferring Failure in a Digital, Globalized World mentions that the security of most valuable information of the organisation depends on the correct processing by the personnel accessing it [6].

The other common source of threat is the false sense of security awareness, which means that the organisation and its senior management believes, that the security of information is complete in the organisation and nothing threatens it, while there are gaps in the security measures and applied information security tools.

2 Data Protection and Data Protection Acts

Most of the organisations uses, stores and processes personal data. Processing and management of personal data shall adhere to the national and international legislation on data privacy. Governmental organisations process personal data, while respect local and international legal requirements of personal data protection as well as the principles of transparency. The Hungarian Act CXII of 2011 on information self-determination and freedom (ISDF) conditions which should be fulfilled by organisations handling personal information. The regulations of ISDF state that steps shall be taken to ensure that the confidentiality of personal information is protected. This Act requires the organisations handling personal information:

- to ask consent of the data subject to use the information for the given purpose;
- to announce the processing of personal information to the supervisory authorities;
- to keep records of personal information handling activities (forwarding and processing);
- to provide information to the data subjects upon their request, about their processed and forwarded data to the processing organizations;
- to ensure that personal data is not accessible by unauthorized persons [7].

The data protection requirements fulfill the principles of confidentiality, so it is closely related to information security. This means that organisations should use all of the available measures to guarantee the confidentiality of the personal data.

In the Hungarian public sector, the implementation of information security is enforced by the Act L of 2013 (ISA) [8] and its implementing regulations, mainly the Ministry of Interior decree 41/2015 (ISAIR) [9] which is based on NIST SP 800 53 [10] and ISO/IEC 27001:2013 [2] standards, but somewhat deviates from their requirements. The ISAIR of ISA focuses on the processed personal data amount when classifying information systems into security classes [9].

In the financial sector, in addition to the bank security and banking privacy legal requirements several standards and frameworks enhance information security. The most important of these are the EN ISO 9001:2015 and ISO/IEC 27001:2013, ISO/IEC 20000-1:2011, PCI DSS (Payment Card Industry Data Security Standard) standards, COBIT 5 developed by ISACA. Opposite to ISO/IEC 27001 standard the application of which is optional in the financial sector, the PCI DSS standard is publicly available and its application is mandatory for every organisation handling credit card data transactions [21].

On the other hand Omar Y. Sharkasi in the article entitled Addressing Cybersecurity Vulnerabilities draws attention to the fact that the legislation emerging all around the world to address information security, put the emphasis on the compliance, but neglect the advisory part. The author refers to the following improvements areas of information security [11]:

- asset inventory and data classification;
- emerging technology risk;
- the effectiveness of risk assessment;
- data residency and cloud computing risk;
- handling of the internal threat;
- end point security;
- dealing with legacy systems;
- file sharing applications;
- maturity of security and remote access;
- cybersecurity test tools.

The national and international standards, legislation and best practices emphasize the risk based protection of information assets and promote the building of an ISMS. To attain this, all data handled by organisation should be collected. Business and operation processes should be analysed in order to identify risks affecting information security. Although the data and organisation processes drive the information security, attention should be paid to the process execution environment: size, location, business strategy, and financial situation of the organisation [12, 13]. The ISMS should be aligned to the business needs, should underpin business process execution, should have sufficient funding and provide adequate security to the organisation.

If the information security is over-regulated by the ISMS, the requirements fulfil the legal and organisational needs, but make expensive the implementation of security measures and execution of business processes.

If the information security regulation provided by the ISMS is weak, compliance with the regulation does not provide the necessary rules to enforce appropriate security for the information assets of the organisation.

The regulation environment of the organisation (legal environment and by-laws of the organisation) influences the boundary conditions of the developed ISMS. It determines the applicable information security classes, the classification rules for data and information systems and the minimum of security measures and assets [9] to be applied. For state and governmental organisations the ISA and ISAIR define the security requirements. For banks and insurance companies the information security requirements are determined by the legal environment of the financial sector.

3 Quality Assurance, Controls and Measures

In several cases participation in tender procedures is limited to organisations having internationally recognized EN ISO 9001:2015 Quality Management Standard [14] certification. For organisations participating in NATO (North Atlantic Treaty Organisation) tender procedures, there are further quality management requirements under the name AQAP (Allied Quality Assurance Publications). This means that organisations having such certificates have a clear advantage compared to those which do not have. Recognizing this advantage, organisations implemented quality management systems and have certified their operations.

The implemented quality management systems usually support not only the business, but the operation processes of organisations too. This usually includes the implemented information systems life-cycle management processes in the organisation. This means proper information handling, to ensure integrity of data necessary for process execution, which is one of the most important components of information security.

COBIT 5 is the leading framework for the governance and management of enterprise IT developed by ISACA [15]. It is built around the idea that the role of IT systems is to enable business processes and generate value for organisations. It is based on the following principles:

- Meeting Stakeholder Needs;
- Covering the Enterprise End-to-end;
- Applying a Single, Integrated Framework;
- Enabling a Holistic Approach;
- Separating Governance from Management.

This framework groups IT governance processes in five domains:

- Evaluate Direct and Monitror (EDM);
- Align, Plan and Organise (APO);
- Build, Acquire and Implement (BAI);
- Deliver, Service and Support (DSS);
- Monitor, Evaluate and Assess (MEA).

The framework uses maturity model to measure the maturity of processes. This model enrols processes in maturity levels:

- 0. incomplete process – no evidence of systematic achievement of the process purpose;
- 1. performed process – the implemented process achieves its purpose;
- 2. managed process – process implemented in managed mode (planned, monitored, adjusted);
- 3. established process – performed process implemented using a defined process;
- 4. predictable process – established process with defined limits to achieve its process outcomes;
- 5. optimizing process – predictable process continually improved to meet relevant and planned business goals.

The maturity level of executed processes reflects the maturity level of the operation and structure of the organisation, which determines the ability to defend itself against information security attacks.

COBIT 5 support information security with the following publications:

- COBIT 5 for Information Security – supports information security with best practices and methodologies regarding daily operations [16];
- COBIT 5 for Risk – helps implementations of risk analisys based on COBIT 5 [17];
- COBIT 5 for Assurance – provides detailed guidance to IT and internal auditors [18].

5 ISO/IEC 20000 standard and ITIL best practices

In case of large organisations the important business processes and services are supported by several IT services. The design, procurement, implementation, operation, continual improvement and professional retirement of these IT services – functions, infrastructure and processes – play an important role in the delivery of supported business services.

The IT Information Library (ITIL) originally developed by the British Government is an internationally accepted collection of best practices regarding IT Service Management (ITSM). It focuses on optimized delivery of IT services, i.e. providing high quality IT services at best prices. Opposed to the standards and

COBIT which define requirements, ITIL provides best practices as implementation guidelines of ITSM, but the ISO/IEC 20000 standards family based on ITIL provides certification possibilities. The ISO/IEC 20000-1:2011 defines the requirements for a service management system [19]. The ISO/IEC 20000-2:2012 provides guidance on the application of service management systems, including best practices for service management processes [20] within the scope of ISO/IEC 20000-1:2011.

Large organisations operate several IT services and maintain a lot of IT assets. To facilitate their IT operation they need an IT asset database and incident tracking system. Several open source and commercial IT systems are available on the market, which support ITSM processes. The usage of these systems facilitate the availability of IT services and improves integrity of information processed by organisations.

7 Relationships of Information Security, Quality Assurance and IT Service Management

In an increasing number of cases information security is regulated by the legal environment. However having ISO/IEC 27001:2011 standard certification it is not mandatory, organisations being certified have a clear business advantage. Because the value creation, high quality and cost-effectiveness of IT services is indispensable in supporting business services, the implementation of COBIT framework and ITIL best practices is straightforward.

Although the presented standards and best practice frameworks support different disciplines, they overlap, but complement each other as well. This interdependence promotes their integrated implementation. The International Standard Organisation recognizing organisations need to comply with more than one management standard, started to align standard structures to each other. To attain this, they proposed new management standard development guidelines and made proposal for common structure schema in the “High level structure, identical core text, common terms and core definitions” [22] published in the ISO/IEC Directives, Part 1, Consolidated ISO Supplement 6th edition 2015.

Regarding information security the following interdependence can be established between quality assurance (EN ISO 9001, AQAP) , ITSM (ISO/IEC 20000, ITIL) and information security (ISO/IEC 27001, COBIT5, ISA) management systems.

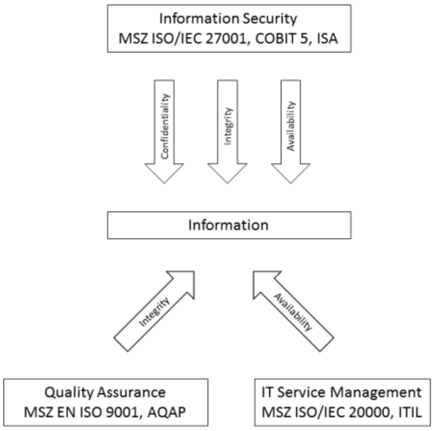

Figure 1.
Interdependencies of insormation security, quality assurance and ITSM

8 Implementation of Information Security

Information security is a dynamic state. It depends on the ISMS and security measures implemented by the organisation. These security measures may consists of: security awareness of employees, implemented by-laws, infrastructure, implemented information systems, etc. To ensure information security changes in business goals, local and international legislation should be taken into account as they affect the services, products, infrastructure and operation of organisations.

The information security is influenced by several factors. The continually changing technology and infrastructure, the daily emergence of new security holes in software, the usage of smart phones, mobile and cloud computing, the widespread of cyber-attacks and advanced persistent threats (APT) constitute serious ongoing risks and present challenges for organisations. Thus periodic analysis of security risks and implementation of security measures do not provide the necessary information security level. To ensure appropriate information security, organisation change management process should be implemented to detect emergence of new security risks and enable implementation of the necessary countermeasures.

Implementation of information security can be achieved using several methodologies. The following chapters describe the most common methods, then an analysis of them outlines their advantages and disadvantages.

8.1 Standalone Implementation of Information Security

In case of standalone implementation of information security based on ISO/IEC 27001 / ISO/IEC 27002 standard, the development of appropriate ISMS plays a central role. To develop suitable ISMS organisations should analyse:

- the structure of the organisation;
- the by-laws of the organisation;
- the data processed by organisation;
- the business processes of the organisation;
- the business support operations processes of the organisation;
- the info-communication and IT infrastructure of the organisation

regarding compliance to the local and international legislation and standards. The ISMS consists of rules and procedures, require security measure implementation to enhance information security. If any non-compliance is found during the analysis, plans should be developed to eliminate the gaps. To develop appropriate ISMS, security measures and operating procedures, organisations should consider the requirements imposed by legislation and standards, technical and financial capabilities of the organisation. Security awareness plays a central role in the implementation of information security too. Beyond security awareness education, employees should be involved in the implementation of security measures, to improve their attitude to information security.

To attain a steady information security state, organisations should implement a cyclic information security planning process, consisting of the following tasks:

- analysis of current situation – gathering of data assets, identification of organisation processes, assessment of information infrastructure;
- threat analysis – identification of relevant threats regarding data, processes and infrastructure of the company;
- suggestions for immediate actions – if there exist threats, which can be handled with minimal resources and efforts;
- risk analysis – analysis of damages (economic, prestige, legal) caused by identified threats in case they realize, identification and ranking of risks, development of risk handling proposals;
- decision on risks to be handled – based on the risk analysis and handling proposals;
- Implementation of security improvement measures.

8.2 Integrated Implementation of Information Security

In several cases organisations have implemented or plan to implement quality management and IT service management systems too. In these cases organisations should consider implementation of the ISMS integrated with these management systems.

ITIL as the best practice of ITSM covers the life-cycle of IT services from the service strategy through service design, service transition, service operation and continual service improvement until retiring them. Its recommendations consider information security and quality management, but does not cover them.

The organisations operating EN ISO 9001 standard based quality management system covering the whole organisation, have quality assurance processes in place for the management of business and operations processes. Their quality assurance activities ensure integrity of the information used in business activities to provide high quality products and services.

In case of organisations which operate quality management and ITSM systems, most of the requirements of ISO/IEC 27001 standard are available incorporated into business, management and operation processes. The requirements not already incorporated in organisation processes, can be easily identified using gap analysis, then implementation plans should be developed to integrate them into the management system of the organisation.

In case of parallel implementation of quality, information security and service management system, considering that International Standard Organisation developed a common management structure schema to support the integrated implementation, development of an integrated management system should be considered first, then filled in with the requirements of the standards.

As the requirements of these standards overlap partially and complement each other, their requirements should be compared and filtered to exclude the redundancy. To support this, correlation, tables were developed which help selection of the requirements which should be implemented. The implementation order of the requirements of standards may be influenced by the legal environment, but should be considered that information security measures are supported by quality and ITSM system processes.

8.3 Process Oriented Implementation of Informtion Security

Because nowadays the operation of business, management and operation processes cannot be imagined without processing, storing and forwarding information, the employees executing organisation processes must protect the information they work with.

In case of process based information security implementation opposite to standalone and integrated implementation methods, the main focus is on information protection during process execution. This brings into the light the quality management tasks based on EN ISO 9001 standard too. During process based implementation it is need for:

- detailed assessment and modelling of business processes [27];
- risk assessment of business processes and ordering them by criticality [26];
- process execution analysis and for process activities [25]:
  - identification of the affected data;
  - determination of the criticality of processed data;
  - determination of the accessible/modifiable set of data for the execution roles [24];
- training data, process and application owners and participants in process execution to protect the processed data;
- preparation of the IT infrastructure and supporting processes to protect the processed data;
- training employees to the secure execution of IT systems supporting organisation processes;
- implementation of ISO/IEC 20000 standard or ITIL based ITSM processes complemented with ISO/IEC 27001 standard requirements;
- development and implementation of the missing ISMS regulations and procedures based on ISO/IEC 27001 or ISA and ISAIR;
- organisation change management process implementation to enable detection of information security risks;
- periodic review of organisation processes information security.

The process oriented implementation of information securtiy, improves IT system security by enabling data protection by design technics [23].

An implemented EN ISO 9001 based quality management system facilitates the information security system process based implementation. It is indispensable the participation of professional process management and IT service management consultants in the implementation. Process management training to the data and application owners is critical to the process based implementation of information security.

9 Commparision of Information Security Implementation Methods

The following table compares the different kind of information security implementation methods advantages and disadvantages.

Method	Advantages	Disadvantages
Standalone	• It is easy to identify the requirements of the standard or law chosen as basis for implementation. • Verification of materialization of the planned security measures is easy. • Lower initial cost.	• Risk that criteria formulated in the ISMS may not realise in practice. • The risk of too strict by-laws, which are: o unenforcable; o obstruct the work; o genetrate additional cost. • Risk that affected employees who does not participate in the development of by-laws, will not comply with them. • Risk that implementation does not address the specific details of the business/ operating processes. • The standard and laws does not provide practical guidance on implementation of security measures. • IT may happen that the implemented security measures does not ensure the necessary protection.
Integrated	• ITIL best practices provide guidance on development and implementation of some security measures. • Verification of the	• The requirements to be applied have to be selected from the requirements of standards and laws selected for implementation. • The inadequately designed and

Method	Advantages	Disadvantages
	planned security measures materialization is easy. • The security measures designed and implemented according to the quality management system meet the expectations.	implemented ITSM processes obstruct the work. • The risk too strict by-laws, which are: ○ unenforceable; ○ obstruct the work; ○ generate additional cost. • Risk that affected employees who does not participate in the development of by-laws, will not comply with them. • Risk that implementation does not address the specific details of the business/ operating processes. • Higher initial cost.
Process based	• With detailed analysis of organisation processes, higher level security level can be attained. • IT is suitable for implementation in small organisations with few processes. • The implementation cost depends on the number of organisation processes.	• In case of large number of organisation processes, the implementation depends more on process owners and participants, so in some conditions it may fail. • The development and implementation of ITIL based support processes is indispensable for a successful implementation.

Figure 2.
Comparision of information security implementation methods

Conclusions

Whatever information security implementation method (standalone, integrated, process based) is selected:

- requirements of standards and laws should be fulfilled;
- management support is critical to achieve the goals;
- supporting stakeholder needs, facilitate implementation of information security;
- ITSM implementation support information security implementation.

Standalone implementation worth considering in the case when no other management standards are implemented nor planned.

The process based information security implementation method:

- uses a bottom-up approach, therefore facilitates realization of higher level security awareness;
- is straightforward to implement in organisations with small number of organisation processes;
- is more challenging to carry out in organisations with large number of organisation processes.

Integrated implementation of information security with ITSM and quality management, support practical IT service management and provides better quality business process support.

References

[1] Information Technology. Security Technics. Information security management systems. Requirements, ISO/IEC 27001:2005, 2005.

[2] Information Technology. Security Technics. Information security management systems. Requirements, ISO/IEC 27001:2013, 2013.

[3] Ernst & Young: Get ahead of cybercrime EY' Global Information Security Survey 2014 (p. 40); http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf (downloaded: 2015.02.27.)

[4] PwC: Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015 (p.42);

http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml# (downloaded: 2015.02.27.)

[5] A Frost & Sullivan Market Study in Partnership with ISC2: The 2013 (ISC)2 Global Information Security Workforce Study (p.28); www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf (downloaded: 2015.02.27.)

[6] Jeimy J. Cano: „The Challenge of Transferring Failure in a Digital, Globalized World," ISACA Journal., vol 5., pp. 37-42, Jun. 2015.

[7] 2011. évi CXII. törvény "Az információs önrendelkezési jogról és az információszabadságról," Magyar Közlöny., vol 88., pp. 25449- 25486, Jul. 2015.

[8] 2013. évi L. törvény "az állami és önkormányzati szervek elektronikus információbiztonságáról," Magyar közlöny., vol. 69, pp. 50241-50255, Apr. 2013.

[9] 41/2015. (VII. 15.) BM rendelet "az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről," Magyar Közlöny.,vol. 103. pp. 17700-17750. Jul. 2015.

[10] Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, 2013.

[11] Omar Y. Sharkasi: "Addrssing Cybersecurity Vulnerablilities," ISACA Journal., vol 5., pp. 19-29, Jun. 2015.

[12] Alan Calder, "Scope definition," in Implementing Informaion Security based on ISO 27001/ISO 27002, 2nd ed. Zaltbommer, Netherlands: Van Haren Publishing, 2009, ch. 11, pp. 35-38.

[13] Alan Calder: "Nine Steps to Success: An ISO 27001 Implementation Overview," 2nd ed., IT Governance, UK, 2013.

[14] Quality management systems. Requirements, EN ISO 9001:2015, 2015.

[15] COBIT 5, ISACA, Rolling Meadows, IL, 2012.

[16] COBIT 5 for Information Security, ISACA, Rolling Meadows, IL, 2012.

[17] COBIT 5 for Information Risk, ISACA, Rolling Meadows, IL, 2013.

[18] COBIT 5 for Assurance, ISACA, Rolling Meadows, IL, 2013.

[19] Information technology - Service management – Part1: Service management system requirements, ISO/20000-1:2011, 2011.

[20] Information technology - Service management - Part2: Guidance on the application of service management systems, ISO/20000-2:2012, 2012.

[21] Payment Card Industry (PCI) Data Security Standard v3.1 Requirements and Security Assessment Procedures, PCI SCC Standard PCI DSS v3.1, 2015.

[22] ISO/IEC: ”High level structure, identical core text, common terms and core definitions,” in ISO/IEC Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, 6th edition, 2015.

[23] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner: Privacy and Data Protection by Design, ENISA, 2014.

[24] Haio Roeckle, Gerhard Schimpf, Rupert Weidinger: Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization, RBAC '00 Proceedings of the fifth ACM workshop on Role-based access control, 2000, pp.103-110.

[25] Rodriguez, Alfonso Fernandez-Medina, Mario Eduardo Piattini: A BPMN Extension for the Modeling of Security Requirements in Business Processes, IEICE TRANSACTIONS on Information and Systems, Vol.E90-D. No.4. 2007. pp.745-752.

[26] Risk management - Principles and guidelines, ISO 31000:2009

[27] Arthur Tenner, Irving DeToro: BPR – Process Redisign.Prentice Hall, 1996.