INFORMATION AND CYBERSECURITY, RISK MANAGEMENT AND AUDIT PROCESS

Barbora Kotkova
Tomas Bata University in Zlin, Nad Stráněmi 4511, 760 05 Zlín, e-mail: b_*kotkova@fai.utb.cz*

Abstract

The contemporary information society is characterized by the use of information and communication technologies (ICT). Management of informatics and its connection to processes in the company is one of the main elements of the management of the organization. Knowledge of the real state of informatics and its functioning with business processes is the main criterion of the development of every company.

The aim of the article is to briefly describe the issues of cyber and information security, risk management, and audit. It includes an analysis of relevant laws and standards related to these topics. The main goal of the article is based on these foundations, and that is the proposal of the cybersecurity audit procedure.

Companies are making every effort to make the most of technology, which means they are highly dependent on ICT. Cyberspace is a place of attack and defense. Companies must be prepared to face possible threats and must take appropriate measures to ensure safety. The purpose of an information security management system is to ensure an adequate level of security and thus be prepared to handle security incidents.

Keywords:. Analysis, Audit, Identification, Information Security, Cybersecurity, Technology, Process, Standard, Management

1. Introduction

The information has its value and importance for those who own it. Information should not be altered, attacked or stolen. At the same time, it needs to be available to anyone who is authorized to work with it. The opposite problem is then denying access to it. Access to information and business processes must be managed based on the requirements of the information security policy and the overall business strategy and policy. All existing technical and technological means of disseminating and authorizing information must be taken into account. [1]

Ensuring security in both information and cyberspace means dealing with threats that take many forms and forms. The development of technologies and the number of devices connected to the network represent a great opportunity for business and services, but at the same time, the potential for abuse, threats and, in particular, their consequences have increased. Ensuring safety is a must and enforced by-laws, directives, and standards. The article includes an analysis of these relevant laws and standards and proposes a cybersecurity audit procedure so that no area is neglected.

2. Information Security

Information security is one of the most important areas of all organizations. The definition of the term information is related to the term data. Data is the expression of facts and ideas in a prescribed form so that they can be stored, transmitted and processed. Information is the result of data processing that has meaning and value for the recipient.

Information security requirements for information security:

- effectiveness - information is delivered in a timely, correct, consistent and usable manner,
- efficiency - information is provided with the most productive use of resources,
- compliance - deals with compliance with laws, regulations, and agreements,
- reliability - refers to the provision of appropriate information for management,
- confidentiality - is the protection of sensitive information from misuse,
- integrity - refers to the validity, accuracy, and completeness of the information
- availability - information is available as needed
- authenticity must ensure the verifiability of the declared origin of the asset.

Thus, information security is a set of measures that protects information from unauthorized use and tampering so that it is available to users who are authorized to work with the information at any time. Information security management is a continuous, repetitive set of interrelated activities.

Unfortunately, “many information systems it was not designed to be safe ', notes the introduction of one of the standards [2] series ISO / IEC 27000. The number of security threats to which organizations are exposed each year

increases so do the amount of malicious code (so-called malware) and cybernetics attacks in general, which affects the Czech Republic, as indeed in his latest report Military Intelligence at the Ministry of Defense of the Czech Republic. [3]

3. Cybersecurity

Cybersecurity is a set of legal, organizational, technical, physical and educational measures designed to ensure secure cyberspace. Cyberspace is the digital environment in which information is generated, processed and exchanged. It consists of information and communication technologies and also includes a connection to a public network (Internet). Furthermore, these are the measures that each company determines according to its needs to create and maintain safety.

The definitions of cyber and information security are not very different. The difference in cybersecurity and information security stems from ISO 27032, which states that information security is concerned with protecting the confidentiality, integrity, and availability of information in general to serve the needs of the users of the information in question (ISO 27032, 2013). While cybersecurity is the preservation of the confidentiality, integrity, and availability of information in cyberspace (ISO 27032, 2013). This implies that cybersecurity is a subset of information security.

Cybersecurity management is designed to minimize threats to the organization. Therefore, it is important to know what threats can affect an organization and what its impact might be. A security threat is a potential cause of an undesirable event that can result in damage to the system and its assets, such as destruction, undesirable access (compromise), data modification, or unavailability of services.

ISO 27000 standards deal with the information security system. The Cyber Security Act, which includes organizational and technical measures, is based on ISO 27001.

ISO 27000 - the document contains a definition of the basic information security terms used throughout the ISO 27000 set.

ISO 27001 defines information security requirements. Here, compliance with the requirements for the establishment, implementation, operation, monitoring, revision, maintenance and improvement of information security management systems is assessed, as well as requirements for security controls. Individual objectives and measures are derived from the following standard.

ISO 27002 - the standard defines information security measures for 35 main categories and contains 114 controls. It is a set of best practices for information security.

ISO 27003 - The standard supports the introduction of an information security management process to assure the other party about risk management within acceptable limits. The standard provides advice on how to develop an ISMS deployment plan following ISO 27001. Other recommendations concern the implementation of the ISMS into the organization. ISO / IEC 27003 was developed to provide support to organizations and recommendations for the implementation of ISMS in accordance with the requirements of the standard ČSN ISO / IEC 27001. [5]

ISO 27004 - focusing on the development and use of metrics, assesses the effectiveness of measures.

ISO 27005 is a standard for information security risk management and recommendations specified in ISO 27001. The subject of the standard issued under ČSN ISO / IEC 27005 are recommendations for risk management in the field of information security. [6]

ISO 27006 - Recommendations for ISMS auditing and certification bodies. It is intended to support the process of accreditation of certification bodies.

ISO 27007 - Recommendations for Audit Program Management and ISMS Audit Areas.

ISO 27032 - Recommendations for improving the state of cybersecurity such as technical measures, preparing for attacks, detecting and monitoring attacks and responding to attacks. It also focuses on cooperation, which must be done safely.

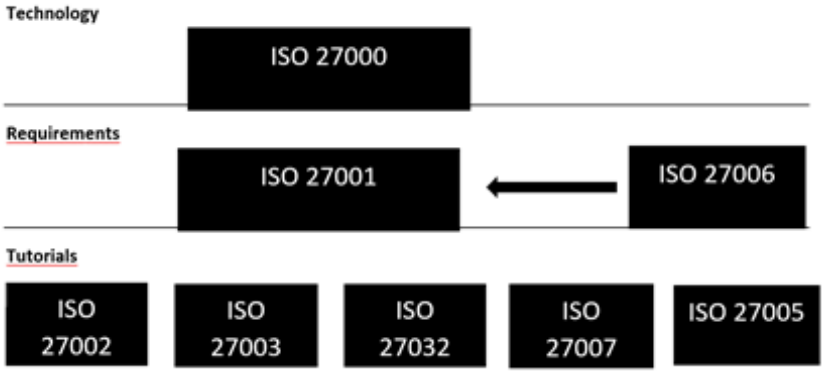

Fig. 1. Correlation of Standards

4. Risk Management

Risk management is a measure set out in the Cyber Security Decree. Risk affects the organization or its components. It also means assets that the owner uses, valorizes and protects. The owner is, therefore, the person charged with managing this asset and overseeing its condition and continuity. He needs to know what risks are threatening him and how to deal with them. Under the Cyber Security Decree, the owner is the guarantor of the asset and has the responsibility to ensure its development, use, and security.

Ensuring the required security status is an expense for an organization, where costs must match both the level of safety and the level of potential damage. Building an information security system must, therefore, be systematic in order to achieve a balance between the costs incurred and the potential damage. The standards of this series are adopted, translated and issued by the Office for Technical Standardization, Metrology and State Testing. [4]

Risk management according to ISO 31000, ISO 27001 and ISO 27005: Risk management and its success depends on the risk management framework used to manage it effectively. Continuous improvement of risk management, determination of risk responsibilities, ability to manage risks is necessary. Communication between all stakeholders of the identified risks and their actions is also important (ISO 31000, 2010). Information security risk management is a coordinated risk management activity (ISO 27005, 2013).

Risk management leads to (ISO 27005, 2013):

- risk identification, risk assessment in terms of their consequences and probability of their occurrence,
- the likelihood and consequences of these risks have been widely recognized,
- the prioritization of risks has been identified,
- managers and employees have been trained in risk management and mitigation measures, introducing processes that "allow authorized persons access to the right resources at the right time and for the right reasons." [7]

Identification and evaluation of assets - ISO 27005 divides assets into primary and ancillary assets (primary assets rely on them). Primary assets are business processes, activities, and information. Supporting assets are hardware, software, networks, workers, employees and more. For risk management, it is necessary to identify all assets and describe their assets. Asset identification is followed by an asset valuation process. The valuation is based on criteria and determines the value of the assets. The value of an asset can be defined financially or qualitatively.

Identification of threats and vulnerabilities - threat identification is based on a list of threats that could potentially threaten assets. Some examples of threats and vulnerabilities are given in ISO 27005. These are examples of technical vulnerabilities where they depend on the criticality of information and communication technologies, money and human resources.

Risk analysis - for risk analysis, it is necessary to know the threats that may exploit any of the vulnerabilities and would hurt assets. Depending on the critical circumstances and the extent of the vulnerabilities, the organization must choose a qualitative or quantitative risk analysis methodology, a combination of the two commonly used in practice. The management of the organization must decide whether to conduct a detailed or basic analysis. In particular, a detailed analysis will provide the basis for the appropriate selection and implementation of security measures.

Risk management - performing a risk analysis is a necessary but not sufficient step. The following is risk management, which can be managed in several ways:

- modification of risks - the adoption of changes or introduction of new measures,
- taking risks - the organization decides that the level of risk is acceptable
- risk-sharing - risk-sharing in cooperation with another party eg insurance
- Avoiding risk - for example by ending high-risk processes. [8]

5. Audit

The audit is an irreplaceable feedback tool for an organization. It maps the relationships between the owners of assets, the environment of the organization, and management. The mission of the audit is to obtain the opinion of an independent and qualified expert. This gives an accurate and up-to-date picture of reality compared to the usual standard. The outcomes are demonstrable, correct and contain recommendations for the development of information security systems. Furthermore, the implementation plan, including description, requirements, time and cost. Subsequently, the expected benefits. The audit output can then be an indicator of necessary changes in the system.

The audit must be carried out in every type and size of the organization, otherwise, there would be no feedback on the state of reality against the plan and design of the desired target state. All types of the audit should follow the ISO 19011: 2002 rules and should follow a pre-approved annual and operational plan. In the case of ISMS, it should include, in particular, a review of the ISMS security and management measures described in the security documentation. [9] The audit should verify their implementation in practice. Small organizations do not have to assign separate departments or internal auditor functions, but it is also necessary to assign an internal auditor function to an employee. The results of audits and spot checks should be discussed with the management at least once a year.

A medium-sized organization is already advised to consider a separate function of an internal auditor, who will also be a security auditor. In this case, too, it carries out planned and random checks according to the annual and operational audit plan. This is compiled taking into account the greatest risks and previous audit findings. In order to achieve better

results, it is recommended to carry out at least once a year a review comparative audit of the state of the ISMS, with respect to the requirements of ISO 27001, with the participation of one external expert consultant. [10]

In terms of the audit process and the auditor's work in the organization, the standard (ISO 19011, 2011) divides the audit into:

- internal audit - provided by the organization itself. There is no requirement that the auditor must be an internal employee. If the auditor is an internal employee, neither the law nor the decree stipulates the necessity of his / her independent position within the organization.
- external audit, supplier audit - it is an audit performed by customers at their suppliers (audit by the other party)
- third party audit - may be performed for compliance auditing or certification purposes.

The role of the auditor - An auditor is a person conducting a cybersecurity audit. To carry out this activity, they must have the necessary training and experience in performing KB audits, at least 3 years. It shall assess the compliance of security measures with legal, internal or other regulations and contractual obligations relating to the critical information infrastructure information system, the critical information infrastructure communication system and the major information system. It identifies enforcement measures, carries out and documents periodic checks of compliance with security policy. The results of these inspections shall be taken into account in the Security Awareness Development Plan and the Risk Management Plan at least once a year. It also covers knowledge of ISO standards (27000 series, 19011 series, 17021 series, 9000 series) and laws and decrees. Furthermore, the protection of personal data and other related laws, knowledge of procedures, processes and methods for assessing, managing, monitoring and measuring information security (ISO 19011, 2011), industry specificities and typical risks, as well as personality and character traits such as (ISO 17021-1, 2016):

- adherence to ethical principles, truthfulness sincerity, honesty, and discretion,
- openness to other opinions, diplomacy, willingness to cooperate,
- attention, responsiveness, flexibility, stamina, determination
- self-sufficiency, professionalism, moral credit.

Undesirable behavior may affect the entire audit. Tensions or some sympathise can then undermine the trust in the auditors and thus the audit itself. A positive relationship between auditors and employees of the organization is always beneficial to the audit process.

Audit and its phases according to ISO 19011- The standard is intended for users who are interested in determining and verifying the actual state of the system, or are subject to contractual conditions or are subject to legislative regulations and regulations. The standard is designed for flexibility in use and introduces risk concepts into auditing management systems.

The audit depends on several principles and principles. These make the audit a reliable and effective tool for management feedback and control. These principles ensure that the audit conclusion is independent.

Principles used by the standard:

- Integrity - the auditor works honestly, conscientiously and responsibly. It demonstrates the competence to carry out an audit, its judgment is not affected. It is directed to the audit objectives and performs everything in accordance with applicable legislation and regulations.
- Fair presentation - all audit findings, reports and conclusions truly and accurately reflect audit activities. It also informs about significant obstacles.
- Professional approach - the auditors perform the tasks entrusted with due care and in accordance with their importance and importance. The decisions they reach shall be duly substantiated.
- Confidentiality - The information that the auditor will come into contact with is confidential. It must not be misused for its own benefit or published, thereby causing damage to the audited company.
- Evidence - the audit conclusions should be verifiable.
- Independence - auditors should be completely independent of the audited organization, maintaining impartiality and avoiding conflicts of interest. Internal auditors must be assured of independence from managerial positions in order to preserve the credibility of the audit.

ISO 27006 specifies which activities are not a conflict of interest and can be carried out by the certification body without disturbing the conflict of interest. (This includes, for example, carrying out training and lecturing activities).

Management of the audit program - the top management of the organization determines the objectives of the audit program according to its own needs. They may be separate, simultaneous or complementary.

The program may include:

- the objectives of the audit program and individual audits,
- scope, number, types, duration, locations, audit schedules,
- management of the audit program,
- audit criteria, audit methods, selection of the audit team, necessary resources,
- processes for handling confidential information, information security and other processes.

Setting the objectives of the audit program respects the relationships with partners, applicable legislation, management requirements, and the consistency between objectives and findings is monitored.

Auditing - the commencement of the audit includes an initial contact with the audited organization, the objectives, and subject of the audit are discussed, ways of communication, provision of information and more detailed information

about the circumstances and particulars of the audit. In the initial phase, relevant documents may be requested to examine them. Examining the documents provides an overview of the scope of the documentation, acquaints with the results of previous audits and provides the necessary information for the preparation of the next audit steps.

The audit itself includes the following activities (ISO 19011, 2011):

▪ introducing participants, including guides, and indicating their roles (the guide is the person who assists the audit team and is appointed by the audited organization), observers (the observer is the person who accompanies the team but does not audit)

▪ confirmation of audit objectives, subject matter, and criteria,

▪ confirmation of the audit plan and any other arrangements with the audited organization, such as the date and time of the closing meeting, any further meetings of the audited team and the audited organization's management, and any subsequent changes;

▪ a presentation of the methods that will be used to perform the audit, including an indication that audit evidence will be based on a sample of available information, an presentation of the organization's risk management methods that may arise as a result of the presence of audit team members;

▪ confirmation of formal communication channels between the audit team and the audited organization, confirmation that the audited organization will be kept informed of the audit process, confirmation of the availability of resources and facilities necessary for the audit team, ▪ confirmation of confidentiality and information security issues;

▪ information on the methods of reporting, audit findings, including any existing classification, information on the conditions under which the audit may be completed, information on the final meeting; information on how to deal with potential findings during the audit; information on any feedback systems from the audited organization on audit findings or conclusions, including complaints or appeals.

During the information collection and validation phase, appropriate and representative information is obtained through an appropriate sampling method (which is in line with audit objectives, scope, and criteria) and is evaluated against the criteria. Non-conformities are also recorded, including evidence showing non-compliance. Non-conformities shall be reviewed in cooperation with the audited organization and the conclusions documented.

Audit Conclusion and Audit Report - at this stage, the audit team acts and examines all information and findings. It compares them with audit criteria and objectives. The output of the audit is a report to be agreed upon and provide recommendations to the audited organization for improvement.

Audit conclusions may include (ISO 19011, 2011):

▪ the extent of compliance of the management system with audit criteria,

▪ the efficiency of implementation, maintenance, and improvement of the management system,

▪ achievement of objectives, coverage of the subject and fulfillment of audit criteria,

▪ root causes of findings.

At the closing meeting, the audit team leader meets members of the management of the audited organization to communicate the conclusions reached. The audit process and its results are compiled into a report containing a comprehensive and accurate audit record, including all the elements of the final report. This report is delivered to the addressees of the audit after it has been approved and approved.

The final report and its content depend on the type of assurance and the expectation of the audited organization. It contains assurances that relate to management objectives. Audit opinion/conclusion - the opinion is mandatory for the audit (examination), other types of assurances do not give an opinion in the report, but conclusions are formulated here. In the case of qualified or negative opinion, there is a recommendation that adds recommendations for corrective action. Management's response follows (part of the final report contains management's expression based on the concept of the final report). The response is then part of the final report as well as the auditor's response.

In the absence of a regulation to disclose a report, the auditing party may not disclose anything; The audit is terminated when all planned activities are completed.

5. Conclusion

From the perspective of the information security management system, security policies, security measures, and security documentation form the pillars of security in cyberspace. [11] The feedback tool is an audit of this system. In addition to security measures, information security management also includes setting security policies and maintaining security documentation. Compliance does not automatically ensure full safety. Greater audit depth is dedicated to controlling security assurance processes through specific measures. The effectiveness and efficiency of the audit processes are verified by checks and testing of the active processes. The audit process carried out in accordance with the above points, in accordance with the relevant laws and standards (which are also included in the article), verifies that the measures taken are effective and that important documents are identified.

6. Acknowledgments

This research was based on the support of the Internal Grant Agency of Tomas Bata University in Zlín, the IGA / FAI / 2020/003 project and the Institute of Safety Engineering, Faculty of Applied Informatics.

7. References

[1] CSN ISO / IEC 27001: 2006 Information technology - Security techniques – Systems of Information Security Management - Requirements, Czech Technical Standard ICS 35.040
[2] CSN ISO / IEC 27002. Information technology - Security techniques - Management procedures information security. Prague: Czech Standards Institute, 2008
[3] MILITARY NEWS, Ministry of Defense of the Czech Republic. Annual Report on Military Activities news for 2012 [online]. [2013] [cit. 2014-02-23]. Available from: http://www.vzcr.cz/shared/clanky/21/V%FDro%E8n%ED%20zpr%E1va%202012.pdf
[4] http://www.unmz.cz/urad/unmz
[5] CSN ISO / IEC 27003. Information technology - Security techniques - Guidelines for system implementation information security management. Prague: Czech Standards Institute, 2011
[6] CSN ISO / IEC 27005. Information technology - Security techniques - Information security risk management. Prague: Czech Standards Institute, 2009
[7] WAGNER, Ray. Identity and Access Management: Key Initiative Overview [online]. Gartner, 2010 [cit. 2014-03-15]. Dostupné z: http://www.gartner.com/it/initiatives/pdf/KeyInitiativeOverview_IAM.pdf
[8] BÍNA, Lukáš. Zavedení systému řízení bezpečnosti informací v praxi. Praha, 2014 [cit. 2018-04-14]. Diplomová práce. Česká zemědělská univerzita v Praze.
[9] Bezpečnostní dokumentace [online]. [cit. 2018-02-24]. Dostupné z: http://www.it-security.cz/sluzby/bezpecnostni-dokumentace.html
[10] ČERMÁK, Miroslav. Řízení informačních rizik v praxi: vysokoškolská učebnice. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.
[11] FLEISCHMANNOVÁ, Veronika. Kybernetická bezpečnost. Praha, 2015 [cit. 2018-04-14]. Diplomová práce. Vysoká škola ekonomická v Praze.