Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методика побудови систем менеджменту інформаційної безпеки підприємств на підставі вимог міжнародного стандарту ISO/IEC 27001:2013
(тема)

студент 2 курсу, групи АМСЗІім-20-1
Згуірі Іссам
(прізвище, ініціали)
Спеціальність: 125Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: завідувач кафедри ІВТ Захаров І.П.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В. В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
«_____» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Згуірі Іссам
(прізвище, ім'я, по-батькові)

1. Тема роботи: Методика побудови систем менеджменту інформаційної безпеки підприємств на підставі вимог міжнародного стандарту ISO / IEC 27001-2013 затверджена наказом по університету від «26» березня 2022р. № 175 Стз
2. Термін подання студентом роботи до екзаменаційної комісії 15.05.2022 р.
3. Вихідні дані до роботи: основні положення стандарту ISO/IEC 27001:2013: методи захисту інформації систем менеджменту інформаційної безпеки підприємств, вимоги до системи управління безпекою; опис методології аналізу ризиків.
4. Перелік питань, що потрібно опрацювати в роботі:

1) Загальні вимоги до системи управління інформаційною безпекою
2) Управління ресурсами
3) Удосконалення СУБД
4) Відповідальність керівництва

5.Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: демонстраційний матеріал у вигляді ppt-презентації;

1. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по-батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Захаров Ігор Петрович		15.05.2022

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	01.03.20220	Виконано
2	Збір матеріалів для дослідження	15.03.2022	Виконано
3	Розробка 1 розділу	25.03.2022	Виконано
4	Розробка 2 розділу	20.04.2022	Виконано
5	Розробка 3 розділу	30.04.2022	Виконано
6	Розробка 4 розділу	10.05.2022	Виконано
6	Оформлення дипломної роботи	15.05.2022	Виконано

Дата видачі завдання 01 березня 2022 року

Студент _____ Згуірі Іссам
(підпис)

Керівник роботи _____ проф. Захаров І.П.
(підпис)

Кваліфікаційна робота не містить відомостей, що заборонені до відкритого друку

студент 2 курсу, групи АМСЗІім-20-1  Згуірі Іссам

Керівник  проф. Захаров І.П

РЕФЕРАТ

Пояснювальна записка: 47 с., 3 рис., 6 табл., 18 джерел.

МЕТОДИКА, МЕНЕДЖМЕНТ, ІНФОРМАЦІЙНА БЕЗПЕКА, АНАЛІЗ РИСКІВ, ВНУТРІШНІЙ АУДИТ

Об’єкт дослідження – системи менеджменту інформаційної безпеки підприємств.

Предмет дослідження – методика побудови систем менеджменту інформаційної безпеки.

Мета роботи – систем менеджменту інформаційної безпеки підприємств на підставі вимог міжнародного стандарту ISO / IEC 27001-2013.

Методи досліджень – аналіз науково-технічної літератури, опис, порівняння, зіставлення, формалізація, розрахунок, побудова моделей, діаграм.

У роботі розглянуті загальні вимоги до систем управління інформаційною безпекою, їх моніторинг і перевірка, вимоги до документації, обов’язки управління, порядок проведення внутрішнього аудиту системи управління інформаційною безпекою підприємства.

Розглянутий приклад внутрішнього аудита системи управління інформаційної безпеки для невеликої організації.

ABSTRACT

The work contains: 47 pages, 3 figures, 6 tables, 18 sources.

METHOD, MANAGEMENT, INFORMATION SECURITY, RISK ANALYSIS, INTERNAL AUDIT

The object of research - information security management systems of enterprises.

The subject of research is the method of building information security management systems.

The purpose of the work - information security management systems of enterprises based on the requirements of the international standard ISO/IEC 27001:2013.

Research methods –analysis of scientific and technical literature, description, comparison, comparison, formalization, calculation, construction of models, diagrams.

The paper considers the general requirements for information security management systems, their monitoring and verification, documentation requirements, management responsibilities, the procedure for conducting an internal audit of the information security management system of the enterprise.

An example of internal audit of information security management system for a small organization is considered.

CONTENT

LIST OF ABBREVIATIONS, SYMBOLS, UNITS AND TERMS

ALE – Annual Loss Expectancy

C – consequence

DMS – Data Management System

DPP – Data Protection and Privacy

EAC – Estimated Annual Cost

ISMS – Information Security Management System

L – likelihood

PDCA – plan–do–check–act

RF – risk factor

INTRODUCTION

An International Standard ISO/IEC 27001-2013 [1] has developed a model for creating, implementing, running, monitoring, evaluating, maintaining, and upgrading an Information Security Management System (ISMS). The implementation of an ISMS should be viewed as a strategic choice for the organization. The design and execution of a company's ISMS is determined by its needs and expectations, security requirements, procedures used, and size. It is envisioned that the supports will evolve over time. It is assumed that an ICSS installation will be downscaled as the organization's needs evolve.

An International Standard [1] is used to check conformity by internal or external parties. It takes a methodical approach to creating, implementing, monitoring, and enhancing a company's ISMS. A company must define and monitor a variety of processes in order to run effectively.

A process is an activity which involves resources and is regulated to change inputs into outputs. One operation's output is commonly utilized as the source input text for the next. A process is the use of a process system inside an organization, and the inspection and monitoring of the operations and interactions.

According to [1], users are invited to emphasize the relevance of the information security management procedure:

a) comprehending a company's security requirements and the need to set information security policies and objectives.

b) establishing and maintaining controls to manage a company's threats and risks

c) monitoring and analyzing the performance and efficacy of the ISMS.

d) continuous enhancement based on objective measurement.

International Standard [1] applies to all organizations (ex: commercial enterprises, government agencies, and non-governmental organizations). It provides the standards for developing, implementing, monitoring, maintaining a documented ISMS

within the context of the organization's overall business risks. It outlines the standards for implementing security measures tailored to the needs of specific companies or portions of organizations. The ISMS is intended to guarantee the selection of suitable and proportional security procedures that safeguard information assets and provide interested parties with trust.

1 INFORMATION SECURITY MANAGEMENT SYSTEM

1.1 General requirements

Within the context of the company's overall business activities and the risks it confronts, the organization must create, implement, operate, monitor, evaluate, maintain, and enhance a documented ISM.

The approach utilized for this International Standard is based on the plan–do–check–act (PDCA) model presented in Figure 1.

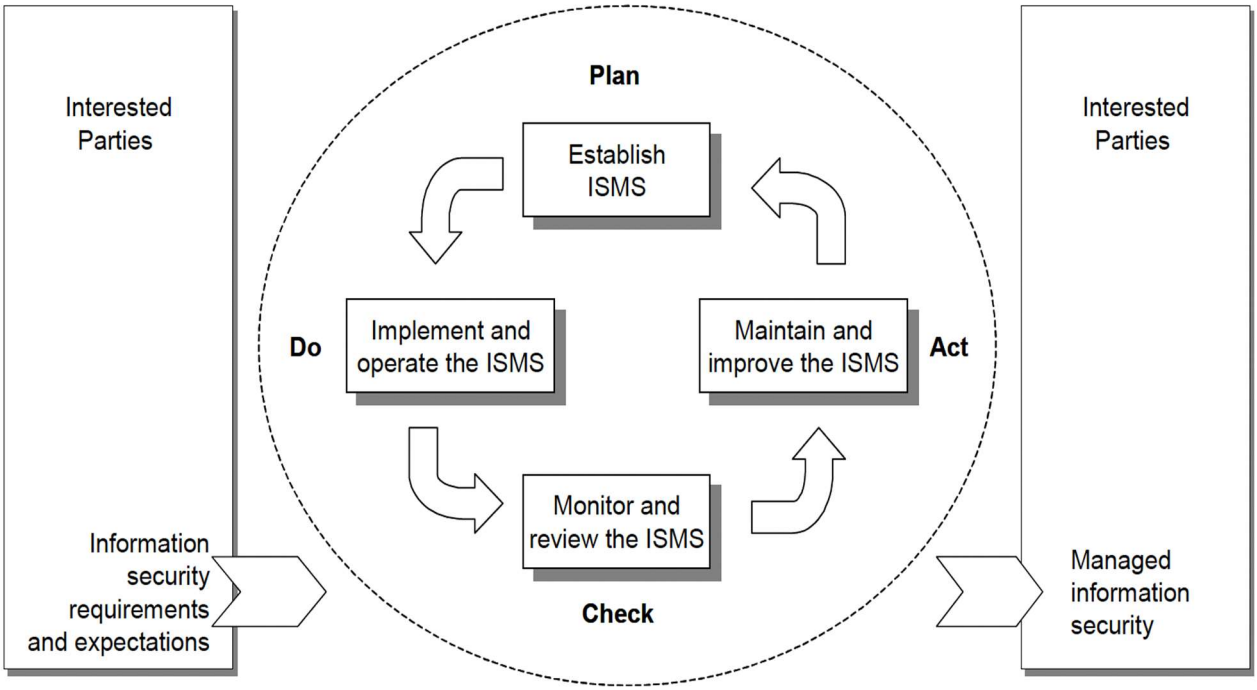

Figure 1.1 – PDCA model applied to ISMS processes

Figure 1.1 shows how an ISMS takes the involved parties' data security requirements and aspirations as input and delivers information security outputs that meet those needs and expectations through required actions and processes.

All ISMS processes in this International Standard are organized using the “Plan-Do-Check-Act” (PDCA) paradigm. Figure 1 depicts how an ISMS takes the interested parties’ information security needs and expectations as input and delivers information security results that meet those demands and standards through the applicable actions and processes.

A criteria could be that breaches involving information security do not lead to severe financial damage or a negative reputation for the firm.

If a severe incident occurs, such as hacking of a company's website, there should be employees with adequate training in proper measures to mitigate the damage.

All ISMS processes in this International Standard are organized using the “Plan-Do-Check-Act” PDCA paradigm (Table 1.1).

Table 1.1 – PDCA paradigm

Plan (establish the ISMS)	Establish ISMS policies, objectives, processes, and procedures related to risk management and information security in order to reach outcomes in accordance with an organization‘s policies and objectives.
Do (implement and operate the ISMS)	Implement and run the ISMS policies, controls, processes, and procedures.
Check (monitor and review the ISMS)	Assess and, if necessary, measure process performance in relation to ISMS policy, objectives, and practical experience, and communicate the findings to management for review.
Act (maintain and improve the ISMS)	Take appropriate mitigating steps based on the results of the internal ISMS audit and comprehensively review, and perhaps other supporting documentation, to enhance efficiency and effectiveness of the ISMS.

1.2 Establishing and managing the ISMS

1.2.1 Establish the ISMS

The following actions must be taken by the organization:

a) Define the scope and constraints of the ISMS in terms of the aspects of the company, the organization, its location, assets, and technology, as well as any exclusions from the scope and their explanation.

b) Define an ISMS policy based on the characteristics of the enterprise, its geography, resources, and technologies :

1) contains a framework for creating objectives, as well as a comprehensive sense of direction with action guidelines for information security;

2) considers corporate, legal, or regulatory requirements, as well as contractual security responsibilities;

3) fits with the organization's strategic risk management environment in which the ISMS will be established and maintained;

4) defines the criteria through which risk will be assessed.

c) Define the organization’s risk assessment methodology:

1) determine an appropriate risk assessment approach for the ISMS and the stated corporate information security, legal, and regulatory needs;

2) create risk acceptance criteria and determine acceptable levels of risk.

The technique chosen for risk assessment must guarantee that risk assessments yield comparable and repeatable findings.

d) Determine the threats:

1) determine the assets covered by the ISMS, as well as the owners of these assets;

2) determine the risks to those assets and their value;

3) determine the flaws that the threats may exploit;

4) evaluate the impact of loss of confidentiality, integrity, and availability on the assets.

e) Analyze and assess the risks:

1) assess the business implications of security failures on the business, taking into consideration the consequences of asset confidentiality, integrity, or availability loss;

2) determine the actual chance of security breaches happening within context of current threats and vulnerabilities, as well as the effects associated with these assets and the measures already in place;

3) estimate the risk levels;

4) using the risk acceptance criteria provided, determine if the risks are acceptable or require treatment.

f) Identify and assess risk-management options. Among the potential responses are:

1) implementing suitable controls;

2) taking risks consciously and objectively, if meet the organization's policies and risk acceptance criteria;

3) attempting to avoid risks;

4) offloading the related business risks to third parties, such as insurance and suppliers.

g) Pick control objectives and controls for risk mitigation:

Control objectives and controls must be chosen and implemented to fulfill the needs indicated by the risk assessment and risk treatment processes. The choices must take into consideration risk acceptance criteria as well as legal, regulatory, and contractual obligations.

h) Seek approval from management for the proposed mitigations.

i) Seek management approval to deploy and maintain the ISMS.

j) Make an Applicability Statement.

A Statement of Applicability must be written, which includes the following information:

1) control objectives and controls already in place

2) the absence of any control objectives , as well as the explanation for their absence.

1.2.2 Implement and maintain the ISMS

The following actions need to be taken by the organization.

a) Create a risk management strategy that specifies the proper management action, resources, responsibilities, and priorities for dealing with information security threats.

b) Carry out the risk treatment strategy in order to accomplish the defined control

c) objectives, which includes finance considerations and the assignment of roles and duties.

d) Put controls in place to achieve the control aims.

e) Specify how the efficacy of the selected controls or groups of controls will be.

f) measured and how these data will be utilized to assess program ’s effectiveness in order to create comparable and repeatable findings.

e) Put in place training and awareness programs

f) Manage the ISMS's functioning.

g) Control ISMS assets

h) Establish processes and other controls capable of detecting and responding to security problems quickly.

1.2.3 Monitor and review the ISMS

The following actions must be taken by the organization.

a) Implement monitoring and review procedures and other controls to:

1) promptly detect errors in processing results;

2) promptly identify attempted and successful security breaches and incidents;

3) allow management to verify whether security actions assigned to people or performed by IT are operating as required;

4) assist in the detection of security events and thus the prevention of security incidents using indicators;

5) decide if the efforts made to remedy a security breach were successful.

b) Conduct frequent assessments of the ISMS's efficacy (including compliance with ISMS policy and objectives and a review of security controls), taking into account the findings of security audits, incidents, effectiveness measurements, suggestions, and input from all interested parties.

c) Assess the efficacy of measures to ensure that security requirements are satisfied.

d) Review risk assessments at scheduled times and evaluate risk exposures and specified acceptable risk levels, considering changes to:

1) the organization;

2) technologies used;

3) business strategy and processes;

4) vulnerabilities discovered;

5) the efficacy of the controls put in place;

6) changes in the legal or regulatory environment, new contractual duties.

e) Regularly conduct ISMS audits.

f) Perform a management assessment of the ISMS on a regular basis to verify that the scope is sufficient and that enhancements to the ISMS process are recognized.

g) Update security strategies to reflect the results of monitoring and evaluating actions.

h) Keep track of any activities or occurrences that may have an influence on the efficacy or performance of the ISMS.

1.2.4 Maintain and improve the ISMS

The organization must conduct the following on a regular basis:

a) Implement the recommended ISMS enhancements.

b) Take necessary corrections and preventative steps, applying experience gained from other companies' and the organization's own security experiences.

c) Explain the actions and improvements to all interested parties in sufficient detail.

d) Ensure that the enhancements meet their targeted outcomes.

1.3 Documentation requirements

1.3.1 General

Documentation must include documents of management choices, activities that can be traced back to managerial policies and decisions, and capable of producing accurate reproducible results. It is critical to be able to demonstrate the link between the selected controls and the findings of the risk assessment and risk treatment process, and from there to the ISMS policy and objectives.

The ISMS documentation must cover the following items:

a) documented statements of the ISMS objectives and policies;

b) the scope of the Information security management system;

c) guidelines and procedures in assistance of the ISMS;

d) a summary of the risk assessment;

e) risk assessment review report;

f) risk mitigation plan;

g) ocumented procedures required by the organization to ensure the effective planning, operation, and control of its information security processes, as well as

descriptions of how to measure control effectiveness;

h) the Statement of Applicability.

1.3.2 Control of documents

Required documents must be safeguarded and managed. A written method must be conducted to determine the management actions required to:

a) confirm documents for adequacy prior to issue

b) monitor and revise documents as needed, and re-approve document;

c) make sure that improvements of documents are recognized

d) guarantee that relevant versions of applicable data are attached

e) guarantee that documents are still legible and easily recognizable

f) guarantee that documents are available to those who need them, and are forwarded, stored, and eventually discarded.

g) guarantee that documents of external nature are identifiable.

h) limit document distribution.

i) avoid the unintended use of old documents

j) apply appropriate classification to old documents if they are maintained for most any reason.

1.3.3 Control of records

Records must be generated and maintained to demonstrate compliance with regulations and the successful operation of the ISMS. They must be preserved and governed. The ISMS must take into consideration any applicable legal or regulatory requirements as well as contractual commitments. Records must be readable, easily recognized, and retrievable always. Controls for record identification, storage, protection, retrieval, retention time, and destruction must be established and

implemented. Records of the process's performance and all instances of serious security events connected to the ISMS must be retained.

2 MANAGEMENT RESPONSIBILITY

2.1 Management commitment

Management must prove its dedication to the organization, implementation, operation, monitoring, review, maintenance, and improvement of the ISMS by:

a) developing an ISMS policy;

b) constructing ISMS goals and strategy;

c) establishing roles and responsibilities for information security;

d communicating to the organization the terms of engaging information security objectives and abiding to the information security policy;

e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;

f) determining the risk acceptance criteria and acceptable riskiness;

g) guaranteeing that internally ISMS audits are conducted;

h) performing management evaluations of the ISMS.

2.2 Resource management

2.2.1 Provision of resources

The company shall assess and to provide the resources required to:

a) define, implement, monitor maintain, and enhance an ISM;

b) guarantee that information security protocols support business needs;

c) address legal requirements and contract terms security commitments;

d) preserve proper protection by successful implementation of all performed controls;

e) write reviews as needed and respond appropriately;

f) Improve the efficacy of the ISMS as needed.

2.2.2 Training, awareness and competence

The company should guarantee that all personnel delegated responsibilities defined in the ISMS are skilled to complete the necessary tasks by:

a) deciding the required skills for personnel able to perform work affecting the ISMS

b) training employees or carrying other actions (for example, employing talented employees) to meet business requirements..

c) assessing the success of activities done;

d) Collecting data of education, skills, training done, expertise, and certifications.

The company must also ensure that appropriate employees are aware of the significance and relevance of their information security actions and how they contribute to the fulfillment of the ISMS goals.

3 INTERNAL ISMS AUDITS

Internal ISMS audits must be conducted periodically by the organization to assess if the control targets, processes, and procedures of its ISMS:

a) meet the criteria of this International Standard and any relevant laws or regulations.

b) meet the specified information security requirements:

i) are implemented and maintained properly;

ii) work as planned.

Such audit program must be established, considering the state and importance of the processes and areas to be examined, as well as prior audit outcomes. The scope, frequency, and techniques of the audit must be determined. The appointment of auditors and the performance of audits must assure the audit process's objectivity and impartiality. Auditors are not permitted to audit their own work.

A written protocol must outline the duties and procedures for planning and performing audits, as well as reporting results and preserving records. The management responsible for the inspected area must guarantee that steps are done as soon as possible to eradicate discovered inconsistencies and their causes. Verification of actions done and reporting of verification findings are examples of follow-up activities.

3.1 Management review of the ISMS

3.1.1 General

Management must conduct an annual evaluation of the organization's ISMS to verify its continued appropriateness, sufficiency, and effectiveness. This assessment will entail examining potential for improvement and the need for modifications to the ISMS, including the information security policy and objectives. The outcomes of the evaluations must be documented, and recordings must be kept.

3.1.2 Review input

A managerial report shall must include following:

a) outcomes of ISMS audit activities;

b) Feedback or suggestions from relevant parties;

c) methods, products, or procedures that can be used in the organization to enhance the ISMS performance and effectiveness;

d) designation of corrective and preventative decisions;

e) security flaws or risks not addressed properly in the prior risk analysis;

f) outcomes from performance measured data;

g) advice regarding improvements.

3.1.3 Review output

The management review's output must contain any behavior and choices relating to the following.

a) Enhancement of the ISMS's performance.

b) A risk assessment and risk recommended mitigations update.

c) Adjustment of procedures and methods impacting information security as required to react to direct or indirect incidents that may have an impact on the ISMS, such as modifications to:

1) business needs;

2) security services;

3) business functions influencing the current business prerequisites;

4) legal and regulatory needs;

5) risk measures and/or risk acceptance criteria

d) Resource requirements.

e) Enhancements to how control efficacy is assessed.

3.2 ISMS improvement

3.2.1 Continual improvement

The company must constantly enhance the efficacy of the ISMS by implementing the information security plan, information security goals, internal audits, evaluation of observed incidents, preventive and corrective measures, and performance reviews.

3.2.2 Corrective action

To prevent recurrence, the business must take steps to eradicate the source of malfunctions with the ISMS criteria. The planned process for corrective measures must include requirements for:

a) identifying malfunctions;
b) calculating the underlying cause of discrepancies;
c) assessing necessity efforts to ensure that discrepancies do not reoccur;
d) deciding and incorporating the remedial steps required;
e) recording outcomes of measures undertaken;
f) analyzing corrective measures taken.

3.3 Preventive action

To avoid any inconsistencies with the ISMS criteria, the business must take steps to eradicate the source of the problem. Preventive measures must be proportionate to the severity of prospective issues. The documented preventative action procedure must include elements for:

a) detecting probable discrepancies and their origins;
b) deciding and performing preventative measures required;

c) deciding and executing appropriate precautions required;

d) documenting outcomes of measures undertaken;

e) evaluating appropriate precautions done.

The company must define altered risks and determine preventative measure needs, with an emphasis on considerably modified risks.

The threat assessment findings will be used to decide the priority of preventative activities.

4 EXAMPLE OF INTERNAL ISMS AUDITS FOR A SMALL ORGANIZATION

4.1 What companies should manage their information security?

It is entirely optional to implement an information security management system based on the ISO/IEC 27001 standard. In this perspective, it is up to the company to determine whether or not to establish an ISO/IEC 27001-compliant management system.

Obtaining this accreditation is an indirect confirmation that the business fulfills the legal system's necessary safety requirements. It is now feasible to identify which firms in the European Union, are or will be obliged to have a part of such an information security system. These are some examples:

1. Providers of critical services, such as power and oil and gas companies, supply chain operator, manufacturing operators, businesses in the air and rail transport sector, finance, medical services, and drinkable water providers.

2. Corporations are actively deciding to establish an Information Security System In order to meet industry-specific standards or to develop consumer confidence.

4.2 Defining an Information Security Management System

It is a good idea to seek the assistance of an information security professional or to use capabilities inside the business and purchase documentation samples as a starting place for the implementation when creating and executing an Information Security Management System. The following ISMS installation stages can be recognized for each of these alternatives (Figure 4.1).

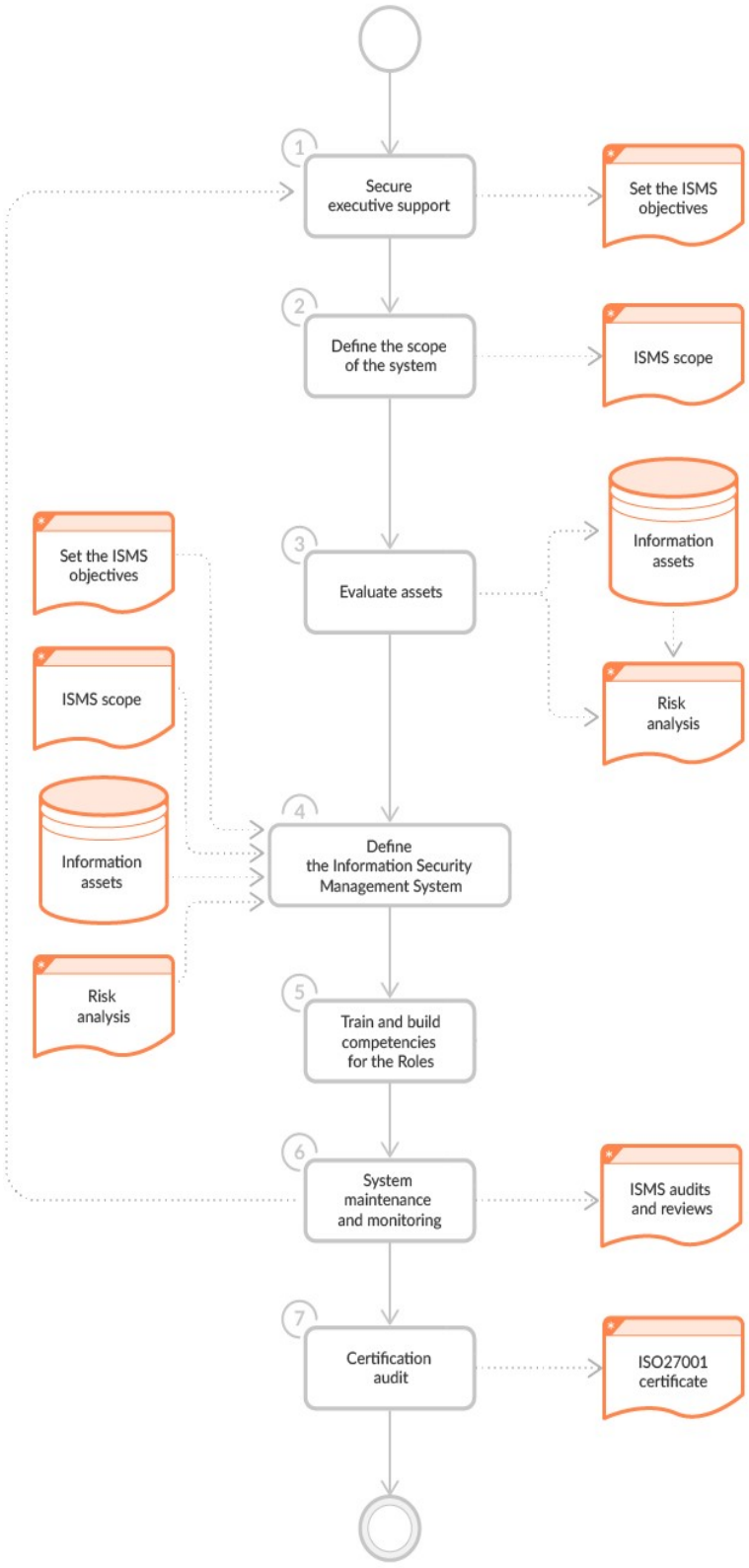

Figure 4.1 – ISMS installation stages

Step 1. Secure executive support and set the objectives

Choosing to deploy an ISO/IEC 27001-compliant ISMS should always begin with obtaining the cooperation / approval of the organization's senior management. This group decides on the distribution of resources and money for developing and maintaining the management program, establishes its goals, and promotes and oversees it within the organization.

Setting goals is an incremental process that requires annual updates. The senior management should set the ISMS objectives, which should match the organization's commercial and legal demands.

Step 2. Define the scope of the system

Despite popular belief, which stems from past experiences with ISO 9001 norms, ISO/IEC 27001 is firmly rooted in the realities and technological needs of information security. This is why, first and foremost, the business should select the security procedures and standards outlined in the standards that directly impact it. The standard describes the procedures that should comprise the organization's Management System, as well as the security protocols that should be established to achieve information security. The outcomes of these actions serve as the foundation for the succeeding phases of implementation.

Step 3. Evaluate assets and analyze the risk

The following stage is to assess data processing assets and do a risk assessment on these. What exactly is asset assessment? It is a review paper that leads in a characterization of the organization’s information processing assets. Among the asset categories are:

1) equipment consists of laptops, telephones, and mechanical data storage

devices;

2) servers – including physical and virtual servers that make up the business's infrastructure;

3) network equipment – components of a firm's infrastructure;

4) cloud services, for example, 365, AWS, AZURE, GOOGLE CLOUD, JIRA, Confluence, Dropbox, banking services, and so on;

5) customer information - information given by customers; generally carries the highest level of company risk;

6) paper data medium.

Those resources that are relevant in terms of information processing should be appraised. This part corresponds to the requirements of the Data Protection Act Regulation (EU) 2016/679, which requires an organization to identify and maintain file systems sensitive classified information.

A risk analysis is performed for each stated asset or group of assets to identify, for example, those associated to the theft of such data. Then, for each asset, an accountable individual is assigned, and a control measure is established.

Step 4. Define the Information Security Management System

At this point in the implementation process, executive endorsement has been obtained, objectives have been established, assets have been appraised, risk analysis results are accessible, and a risk management strategy is in place. As a consequence, the remaining aspects of the Information Security Management System may be specified, and security measures in the company can be applied. This is often an iterative process in which the main ISMS elements are described:

1. Policies;

2. Processes and Procedures;

3. Normative sources;

4. Guides and Training;

5. Instructions;

6. Roles.

This scope of operations is often carried out by a consultant; in any event, the management system should mirror the real processes inside the business while also providing the relevant documentation when appropriate.

Documentation definitions might describe who in the company will be in charge of the specific documentation. During every system maintenance and constant improvement phase, they will be able to maintain and updating data, as well as sending it on to other individuals within the company, in collaboration with the working group.

Step 5. Train and build competencies for the Roles

The company should describe the qualities and skills of the individuals participating in the ISMS at this stage. Following the definition of the ISMS, the first step is to explain it and alert the company about the scope and method of the ISMS functioning, as well as how each employee influences information security. This component should be included into the organization's management system by identifying roles, competences necessary for the jobs, and the method of imparting this expertise on to new workers and renewing it in employees who have previously been taught. It is now time to define the training, guidelines, and competency profiles for each position.

Some of the most common information security jobs seen in most implementations are:

- Employee – role indicating any individual hired by the business;
- Internal auditor - required to perform management system audits;
- IT administrator – reflecting personnel in charge of the organization's IT infrastructure;

- Top management – job that represents the group that is in charge of determining the organization's direction and controlling it at the highest level;
- The Personal Data Protection Regulation (EU) 2016/679 i states that a DPO must be appointed, as in Data Protection Officer.

Step 6. System maintenance and monitoring

Before beginning the certification process for the ISMS, it should be operational in the organization. A fully defined system should have been installed and enforced in the institution for at least a couple of months prior to the beginning of the certification audit, allowing time for undertaking the training required, conducting a management system review, utilizing the security mechanisms, and adjusting the risk assessment and mitigation strategy. During this time, the initial steps outlined in the system management and safety management strategy should also be completed.

When the certification audit begins, the company will have the paperwork and execution records to demonstrate that the ISMS is properly implemented and secure. It should be noted that the capacity to assure constant improvement through tracking, monitoring internal audits, reporting countermeasures, and structured management system evaluations is a basic prerequisite for every management system.

Step 7. Certification audit

A certificate of compliance with the ISO/IEC 27001 standard confirms a company’s installation of an information security management system. The certification involves passing a certification audit conducted by a management system certification agency. The certification audit is divided into two stages. Phase I typically entails a review of the ISMS's breadth and completeness, i.e. a formal evaluation of the

needed aspects of a management system, whereas phase II verifies if the system has been implemented in the organization and truly conforms to its activities.

The organization receives ISO/IEC 27001 accreditation after successful completion the certification process audit. As confirmed, the ISMS must be maintained and upgraded in order to be maintained.

4.3 Maintenance and continuous improvement

The business has already received ISO/IEC 27001 certification. Following the certification audit, top management may presume that the fundamental assets associated with the collection of personal data and data have been recognized, risks have been identified, and adequate security measures to solve the major risk have been implemented. Does this imply you can sit back and relax? No way, no how. In truth, the daily task of ISMS has indeed recently begun. People participating in the operations and security procedures will give suggestions for improvement and modification. The firm will discover which security precautions and procedures need to be improved by performing management system audits. As part of the strategic management system review, the findings of current operational monitoring and system status will be given to senior management.

The ability of any management system to continuously improve and respond to the changing internal and external circumstances of the business is the most significant component of it..

4.3.1 Benefits from the Information Security Management System

What are the advantages of adopting and certifying an ISMS for a company?

1. The organization established and executed a management system by training staff, raising awareness, implementing appropriate security measures, and

implementing a methodical approach to information security management.

2. The possibility of information loss or illegal access.

3. Development of information security professionals' awareness and abilities.

4. Customers’ confidence is increased by proving that the organization is ISO/IEC 27001 certified.

5. The business complies with all regulatory standards, including those outlined in:

- PDPR = Personal Data Protection Regulation (EU) 2016/679,
- cyber-security directive (EU) 2016/1148.

4.4. Building an ISMS Private healthcare organization

This project will discuss an example of how to build a robust information security management system for a healthcare organization. The results will be as the following:

- Creation of an audit checklist in accordance with PDP - personal data protection legislation.
- Risk analysis design and risk reduction approaches.
- External audit of DMS – Data management system

4.5 Steps to establish ISMS for this example

- Identify the scope of the ISMS with respect of the company's traits, location, assertions, and technologies involved.
- Define an ISMS policy.
- Define a systematic approach to risk assessment.
- Identify the risks.
- Risk assessment.
- Identity and evaluate options for the treatment of risks.

- Choose control objectives and risk control mechanisms;
- Create an applicability statement.

4.6 Implementation of ISMS for personal data protection

ISMS requires the development of a security management system centered on personal data protection. As a result, ISMS standards (for example, ISO/IEC 17799) may be used to data management security.

The organization‘s ISMS needs are to create, implement, maintain, and constantly enhance documented ISMS, in this instance DMS is focused on sensitive personal data protection within the framework of the company’s broader business operations and risk (Table 4.1).

Table 4.1 – PDCA description for ISMS

PDCA	Description
Plan	Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and projective
Do	Implement and operate the security policy, controls, process and procedures
Check	Asses and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review
Act	Take corrective and preventive actions, based on results of the management review, to achieve continual improvement of the ISMS

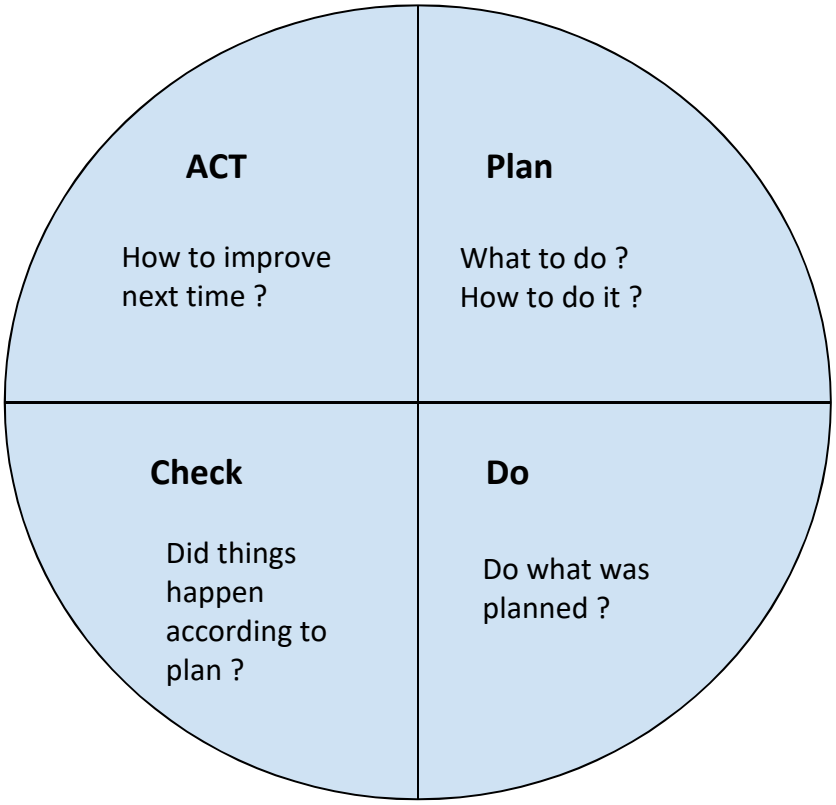

Fig 4.1 – The PDCA model applied to ISMS process

The steps to establish the ISMS are:

- define the scope of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology;
- define and ISMS policy;
- define a systematic approach to risk assessment;
- identify the risks;
- risks assessment;
- identify and evaluate options for the treatment of risks;
- select control objectives and control for the treatment of risk.

4.7 Risk analysis

Risk analysis is the most important phase of ISMS establishment, that is the process which compares assessed risks with benefit and price of possible security control. Standard ISO/IEC TR 1335 [5] defines four possible ways of risk analysis. We chose informal access. Advantage of this access is speed and financial modesty base of risk analysis is fulfillment of following activities:

- threats identification;
- estimation of threat likelihood;
- identification of assets;
- rating of assets;
- determination of vulnerabilities;
- calculation of expected losses at threat impact;
- evaluation of risk analysis.

The interrelationships in risk management are shown in Fig. 4.2 this diagram helps us to understand analysis.

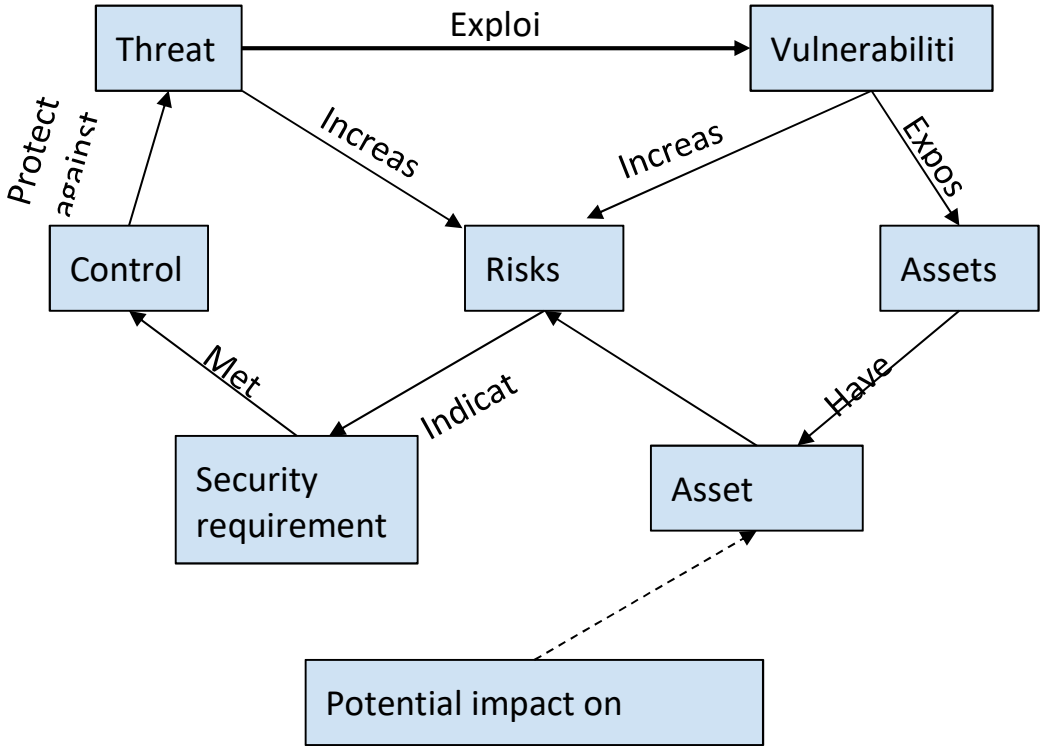

Fig. 4.2 – Diagram of interrelationship in risk management

4.7.1 Risk analysis key terms

The major analysis key terms are:

Risk: The change or likelihood of an undesirable event occurring and causing loss or harm. Note that the key element of risk is uncertainty, without which there is no “Risk”.

Risk analysis: The process of gathering and analyzing risk-related information in the preparation of a risk assessment.

Risk assessment: A detailed articulation of the risks associated with the information assets and supporting ITC resources at risk, threats that could adversely impact those assets and vulnerabilities that could allow those threats to occur with greater frequency or impact.

Threat: A potentially undesirable event that could result in loss or harm. The experience of threat event and its measurable loss or harm is distinct from potential threat events and associated estimates of loss or harm the aggregation of threat-event experience data provides the basis for estimating expected threat-event loss or harm in the future.

Vulnerability: A lack or inadequate application of a safeguard or control that allows a threat event to occur with greater frequency or impact.

Probability: Measures the chance or likelihood of an outcome or event occurring within a finite universe of possibilities or time between 0 and 1.

Uncertainty: The central issue of risk and risk metrics, reflected as the level of confidence, from 0 to 100%, that the associated numbers - and derived results are credible and useful, failure to integrate uncertainty into risk analysis and assessment approaches reduces the credibility of their results.

Quantitative risk analysis: it employs 2 fundamental elements: the probability of an event occurring and its loss.

Quantitative risk analysis makes use of a single figure produced from these

elements, this is called the “Annual Loss Expectancy (ALE)” or the “Estimated Annual Cost (EAC)”, this is calculated for an event by simply multiplying the potential loss by the probability.

It is theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.

The problems with this type of risk analysis are associated with unreliability and inaccuracy of the data Probability can rarely be precise and can in some cases promote complacency. In addition controls and counter-measures often tackle a number of potential events and the events themselves are frequently interrelated, a lot of organizations successfully adopted Quantitative Risk Analysis.

Quantitative risk analysis: This is by far the most widely used approach to risk analysis, Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of number of interrelated elements:

- Threats => these are things that can go wrong or that can “attack” the system examples might include fire or fraud, threats are ever present for every system;
- Vulnerabilities => these make a system more prone to attack by a threat or make an attack more likely to have some success or impact; for example, for fire vulnerability would be the presence of inflammable materials like papers or walls built from wood;
- Controls

Next are countermeasures for vulnerabilities:

- Deterrent controls reduce the likelihood of a deliberate attack
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventive or corrective controls.

4.7.2 Risk analysis methodology description – case study

Results of audit made the base for design of the risk analysis methodology.

The methodology combines the basic principles of quantity risk analysis with qualitative risk analysis. The principles of failure modes and effects analysis (FMEA) analysis can be applied for the methodology design too.

The basic idea of this methodology is:

1.The risks are generated by the processes in the organization. That means that we can search the risks in the processes which process the private information about patients and about organization (transfer, records, liquidation, storage, etc.)

2.The processes are part of an asset in the organization. An object makes the assets of an organization and contains the processes which process the information.

An example of risk analysis results is summarized in the risk analysis forms (Table 4.2 and Table 4.3).

The risk analysis form (Table 4.2) uses those terms:

1. **Process** - Activities in the scope of an object
2. **Risk** - Description of a given risk
3. **Risk code** - Number of risks
4. **Risk assessment** - risk assessment contains three date:

   Consequence => C

   Likelihood => L

   Risk factor => RF

Next columns in the form (Table 4.2) show the current safety precaution and control method of process (internal documentation for process control)

Table 4.2 – Risk analysis form - example of asset risk analysis

Asset	Information system						
Process	Risk - identification of undesirable event	Risk Code	Risk assessment			Current safety precaution	Control method
			C	L	RF		
IS administration	Creation of uncontrolled back-up and database during IS implementation	1.01	32	10	320	No	No
	Backup media loss	1.02	16	5	80	Storing backup media into a safe place	Documentation for data administration procedure
IS operating	Fire (over heat)	1.03	8	5	40	NO	NO
Object risk factor average: 147 Risk assessment summary (risk class): Risk class 2 that means increased risk level. The increase of Standards and monitoring of security process is recommended							

Risk Consequences. In Table 4.4 a review of the impact, the consequence is calculated as a quadrate of risk level (this is the expression of the risk intensity in accordance with impact and level). And the table uses the description and characterization of impact to the healthcare organization, the next table will evaluate the consequence risk.

Likelihood measures the change or probability of an outcome or event occurring within a finite universe of possibilities or time, we can estimate the likelihood on experience and knowledge basis or from records of incidents and events, the Table 5 shows the likelihood of incident or event in fifth difference level. The different levels reflect the weight of likelihood for the risk factor calculation.

Table 4.3 – Risk analysis form – example of asset risk assessment

Asset Risk assessment summary				
Asset Code	**Name**	**Asset risk factor average**	**Risk class**	**Asset value**
0.1	Information system	147	2	7500
0.2	Physical network devices and architecture	20	1	1500
0.3	Doctors desktops	170	2	2500
0.4	Main Server	250	3	3700
0.5	Patient card index	35	2	10750
0.6	Archive	130	2	17000
0.7	Server room	120	2	500
0.8	Work room	50	2	1200
0.9	Laboratories	15	1	6500
0.10	Medical offices	10	1	6800
	Average	109	2	88750 EUR
Value are determined from accounting system as investment and overhead cost				

Risk factor (RF) is the numeric value of a risk. Risk factor is the product of likelihood (L) and consequence (C) calculated by the given equation: $RF = L \cdot C$.

Table 4.4 – Impact review

Level	Consequence	Characterization	Impact description
1	1	insignificant	Insignificant infringement of operating procedure in the organization with immediate correction, 0 financial loss
2	4	Minor	Low financial loss, infringement of operating discipline, infringement of operating instruction sin the IT/SI area
3	8	Moderate	Unauthorized operating with information in the organization infringement of security policy and legislative rules, major financial loss, decrease of patients
4	16	Major	Damage to the goodwill, major decrease of patients, major financial loss, escape insignificant information outside organization, wilful infringement of operating discipline, uncontrolled and unauthorized operating with information and data outside organization
5	32	Catastrophic	Enormous financial loss, heavy decrease of patients, escapes sensitive information and personal data about patients outside organization, permanent damage to the organization

Table 4.5 – Risk Likelihood

Risk likelihood	Weight
Practically impossible incident or event	1
Uncommon incident or event, but coming in specific situation	5
Possible incident or event, incident or event was identified before	10
Frequent incident or event	15
Very often recurrent event and incident	20

CONCLUSION

The risk analysis is simple methodology developed for risk assessment and risk management as part of implementation of ISMS in the healthcare organization

The example of the risk analysis is shown in the risk analysis forms (Table 4.2 and Table 4.3), the goals of action plan are elimination of risks with high risk factor.

The elements used in accordance with ISO/IEC 17799 [6] which were applied for the patient's information system.

REFERENCES

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.

2. ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security.

3. Quality management systems – Fundamentals and vocabulary.

4. Information technology – Guidelines for the management of IT Security – Management guidance on network security.

5. ISO/IEC TR 1335. Information technology – Security techniques – Management of information and communications technology security.

6. ISO/IEC 17799:2005 – Security techniques.

7. ISO 9001:2000. Quality management systems – Requirements.

8. ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.

9. ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security.

10. ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards.

11. ISO 14001:2004, Environmental management systems — Requirements with guidance for use.

12. ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management.

13. ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing.

14. ISO/IEC Guide 62:1996, General requirements for bodies operating

assessment and certification/registration of quality systems.

15. ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards.

16. OECD, Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org.

17. NIST SP 800-30, Risk Management Guide for Information Technology Systems.

18. Deming W.E., Out of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 1986.