POLITECNICO DI TORINO

Master's Degree Course in Computer Engineering

Master's Degree Thesis

Towards standardization of audit procedures for the new version of ISO/IEC 27002

Internal supervisor
Prof. Cataldo Basile
External supervisor
Dr. Fabio Guasconi

Candidate
Maria Luisa Morello

Academic Year 2021-2022

To my beloved sister, my awesome parents and my amazing supporters' grandparents

Acknowledgements

I would like to express my gratitude to my internal supervisor Prof. Cataldo Basile for his availability during this project and throughout my academic career. I would also extend my sincere thanks to my external supervisor Fabio Guasconi, who offered me his assistance and valuable experience throughout the thesis work.

I am deeply grateful to my sister Alessia, the half of my heart, and my best friends, especially Teo, for their unwavering continuous support. I wish to extend my special thanks to all my family, especially to my parents Danila and Aldo, who have always guided me to choose what was the best for me, and my grandparents Maria and Manlio, who have never stopped supporting me simply because they love me and believe in me. In the Turkish language, there is a way used to thank someone that fully represents my feelings for those people who are part of my daily happiness and make my life special, it can be translated as "I am so glad to have you": İyi ki varsın!

Contents

List of Tables v

List of Figures vi

1 Introduction 1
- 1.1 Thesis Outline . . . 2

2 The ISO/IEC 27000 family 4
- 2.1 Introduction . . . 4
- 2.2 Information Security Management System . . . 5
- 2.3 ISO/IEC 27001 . . . 6
- 2.4 ISO/IEC 27002 . . . 7
  - 2.4.1 History . . . 7
  - 2.4.2 Evolution of its controls . . . 8
  - 2.4.3 The new version . . . 8
- 2.5 ISO/IEC 27008 . . . 10

3 Audit process 11
- 3.1 What is an audit? . . . 11
  - 3.1.1 Types of audits . . . 12
- 3.2 Principles . . . 12
- 3.3 Audit evidence . . . 13
  - 3.3.1 Types of audit evidence . . . 14
- 3.4 Audit procedures . . . 15
- 3.5 Audit results . . . 17

4 Design of audit procedures 19
- 4.1 Overview of the current scenario . . . 19
  - 4.1.1 Context of application . . . 19
  - 4.1.2 Problem definition . . . 19
- 4.2 Goal of the proposed solution . . . 20
- 4.3 Preliminary work . . . 20
  - 4.3.1 Workplan and adopted strategy . . . 20
  - 4.3.2 PCI DSS as a reference . . . 21

4.4 Structure of a test procedure . . . 23
4.4.1 Interview . . . 24
4.4.2 Documentation . . . 25
4.4.3 Configuration . . . 25
4.4.4 Observation . . . 25
4.5 Strategy of development . . . 26
4.5.1 Main principles . . . 26
4.5.2 Combination strategy . . . 26

5 Implementation of audit procedures 28
5.1 Organizational controls . . . 28
5.1.1 Introduction . . . 28
5.1.2 Audit procedures . . . 29
5.1.3 Considerations . . . 40
5.2 People controls . . . 40
5.2.1 Introduction . . . 40
5.2.2 Audit procedures . . . 41
5.2.3 Considerations . . . 43
5.3 Physical controls . . . 44
5.3.1 Introduction . . . 44
5.3.2 Audit procedures . . . 44
5.3.3 Considerations . . . 49
5.4 Technological controls . . . 50
5.4.1 Introduction . . . 50
5.4.2 Audit procedures . . . 50
5.4.3 Considerations . . . 61

6 Conclusion 63
6.1 Review and final version . . . 63
6.2 Future use as contribution to ISO/IEC 27008 . . . 64

A Organizational procedures 65

B People procedures 76

C Physical procedures 78

D Technological procedures 80

List of Tables

2.1 Evolution of the number of controls in ISO/IEC 27002 8
4.1 Application pattern of testing methods in PCI DSS standard 22

List of Figures

2.1 ISMS family of standards relationships [6] 5
3.1 Reliability of audit evidence [15] 14
3.2 Process of collecting and verifying information [5] 16
4.1 Combination of four testing methods 23
4.2 Design of the audit procedure structure 23

Chapter 1

Introduction

Information technology had an increasing significance in the industry world over the years. The integration of advanced technologies, methods designed for business and intelligent data management have contributed to make information technology a fundamental part of the operational core of companies. In particular, the utilization of open networks like Internet for internal and inter-organization data transfer has increased the organizations' exposure to information security risks and, consequently, has introduced the need of adequate security measures. The protection of information and related systems is covered by several international standards, so typically organizations decide to resort to the ones of their interest in order to put the effort where considered relevant for their own business. For this purpose, the ISO/IEC 27000 family is the reference set of international standards for information security: it provides requirements and guidelines that can be followed to build a secure system. Differently from other standards like the PCI-DSS which has specific high-security application, ISO/IEC 27000s are not mandatory. However, their fulfillment reduces information security risks and it gives a systematic approach to the management of several information security aspects, which is why they are widely adopted.

Specifically, ISO/IEC 27001 is one of the pillars of the family because it defines the requirements that should be addressed to build an information security management system and, ones companies have implemented them, they can decide whether to obtain a certification against the standard. This process requires an accredited certification body that reviews the entire documentation related to the information security management system and verifies that the related controls, listed in the Annex A of ISO/IEC 27001 and explained in detail in ISO/IEC 27002, have been effectively implemented. Afterwards, audit activities are carried out to verify the procedures in practice and, if the certification body is satisfied, then it will issue the certification. [2, 14]

Audit consists of several systematic activities aiming to check whether practices adopted by a company are in compliance with organizational policies and procedures as well as national and international standard requirements. The role of the auditor becomes crucial since it is a complex activity with a remarkable subjectivity margin and the obtained results determine whether the company satisfies the standard or not. Typically they

analyse documentation, procedures, policies and the decision between compliant and non-compliant evaluation is based on their own experience. This is the reason why guidance such as ISO/IEC 27007 and ISO/IEC 27008 on how to review and assess information security controls are essential for performing an audit as much objective as possible. However, the actual ISO/IEC 27008 does not provide a detailed procedure for each security control to be verified: this could lead to evaluations performed by distinct auditors that can vary from each other and have different accuracy. The great relevance of this gap is evident from both national and global statistics about the number of organizations that resort to such certification. This issue strongly affects the actual scenario: every year at least 44500 organizations are certified with respect to the standard worldwide and over 1500 in Italy [10]. Therefore, the purpose of this thesis work was definitely devoted to solve this gap by defining procedures used during audits for testing the actual implementation of information security controls. [14]

The thesis presents the analysis of the reference standards, the design choices and their motivation, and further considerations over the developed audit procedures and their future utilization. To achieve this objective, first of all, the guidance of ISO/IEC 27002 (Information security controls) and the procedures of PCI-DSS standard have been analysed in order to understand how each control should operate and how its verification should be performed. Hence, a suitable structure of the audit procedure has been defined by employing four audit methods, and an initial version of audit procedures for all controls has been developed accordingly. In the following step, it has been reviewed by aggregating some of the procedures in order to improve and optimize their applicability. As a final result, a table of audit procedures has been generated, ready to be sent over as contribution for the guidance of ISO/IEC 27008 standard.

1.1 Thesis Outline

- Chapter 1 is a introduction of the actual context where the work of thesis has been developed, and for which purpose.
- Chapter 2 introduces the ISO/IEC 27000 family and the standards concerned in the thesis work.
- Chapter 3 introduces the concept of audit through some basic definitions and typical classifications of the audit activity, audit evidence and audit results.
- Chapter 4 analyses the design process of developed procedures. Initially it explains the definition of the problem that the thesis work is intended to solve and then it introduces the approach with which useful documentation has been analysed, especially a well-known example of standardized audit procedures taken as a reference both in design and implementation phases.
- Chapter 5 follows the controls grouping scheme used by the ISO/IEC 27002 document in order to present the developed audit procedures through an analysis of controls' purposes, required protection measures and related activities to be performed by the auditor for verifying their implementation.

- Chapter 6 shows the final result obtained by the thesis work and introduces a possible future use of the developed procedures towards the standardization of the assessment of information security controls.
- Appendix A contains the main organizational controls audit procedures
- Appendix B contains the main people controls audit procedures
- Appendix C contains the main physical controls audit procedures
- Appendix D contains the main technological controls audit procedures

Chapter 2

The ISO/IEC 27000 family

This chapter introduces the 27000 family and the related standards concerned in the thesis work.

2.1 Introduction

The ISO/IEC 27000 family, also referred as 27000 series or ISMS family, is a collection of information security standards defined jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The two organization are the leading issuing bodies for international standards and in the electronics technologies sector, respectively. Basically, this family provides a set of requirements and guidelines that help companies to adopt adequate measures of information security in a systematic manner. In order to reflect the ongoing evolution of the security environment, standards are submitted to the Systematic Review process [8] which is launched whenever necessary or it is automatically performed a predefined number of years after the publication or confirmation, depending on the type of standard.

One of the main reasons of the wide adoption of the 27000 series is its range of applicability: organizations of all sizes, sectors, and types may decide to comply with those standards of their interest depending on their own business requirements, objectives and policies. Thus, with a certification against an internationally recognized standard, on one side providers of products and services enhance their reputation and, on the other side, customers' trust is promoted. This increases the organizations' possibility of expanding sales to international markets since the scheme is universally recognized.

The reference document that gives an overview of the whole family is the ISO/IEC 27000. It provides explanation of the purpose and scope of each standard and it includes many basic terms and definitions. Specifically, it describes the key concept of Information Security Management System that will be presented in the next subsection. As suggested in the ISO/IEC 27000 [6], the standards of the family can be grouped in four thematic macro-areas where vocabulary, requirements, general guides and industry guides are defined. The main standards that can be associated to each category are classified in figure 2.1. Specifically, the three standards considered in the work of the thesis are 27001,27002

and 27008. [14, 2]

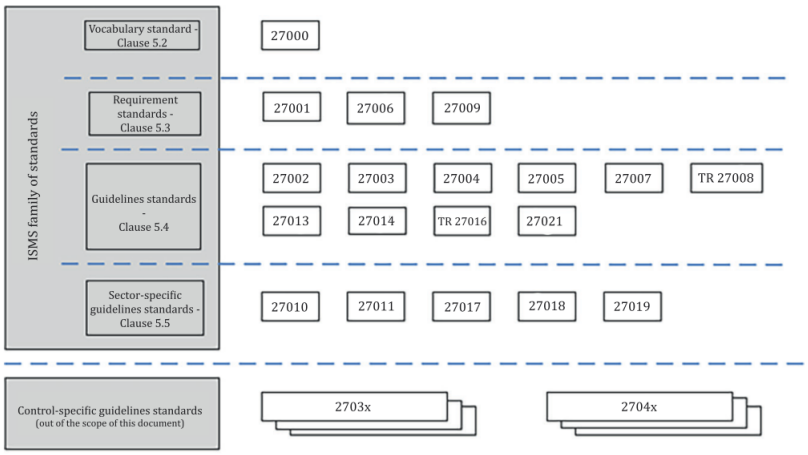

Figure 2.1. ISMS family of standards relationships [6]

2.2 Information Security Management System

As stated in the 27000, *"An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets"*. It means that the organization needs to properly plan how to address every aspect involving information security by implementing a system that minimizes the risks while reflecting objectives and interests of the organization itself. First of all, an information is considered an asset whenever its value requires a kind of protection that should be established and implemented according to the used media of the information itself. By way of example, a confidential document in material or digital format should be accessible only to who has the right and its storage and transmission should be securely managed as well. Following the definition of the information security, the objective is ensuring confidentiality, integrity and availability properties by means of appropriate controls.

The overall approach of an ISMS aims initially for establishing, implementing and operating while later for monitoring, reviewing, maintaining and improving the information security of the organization over the time. Practically, four steps should be undertaken:

1. Information assets and their associated information security requirements are identified. To this purpose, the ISO/IEC 27001 standard provides the requirements for an ISMS and a set of security controls listed in its Annex A. In this phase, business needs and legal, regulatory and contractual requirements are considered as well.

2. Information security risks are assessed and treated.

- Risk assessment is performed through risk analysis and risk evaluation: risks should be identified and prioritized according to the risks acceptance criteria defined by the organization. In this phase, the ISO/IEC 27005 is the reference guidance about information security risk management.
- Risk treatment concerns those risks previously identified and relative decisions should be taken to reduce the overall risk. This can be obtained by selecting appropriate controls to be implemented.

3. Information security controls to be applied are selected based on results obtained from the previous steps. This is the most crucial single step for an ISMS because controls are included or excluded from the scope. Specifically, the ISO/IEC 27002 standard groups a detailed collection of controls acknowledged as best practices. Since it is a general guidance, it can support a variety of organizations but there is also the possibility of not applicable or practicable controls. In these cases, further controls should be introduced.

4. Maintenance and improvement of the ISMS is undertaken through monitoring. Objectives and policies, as well as controls effectiveness are supervised and related results are used to identify possible corrective, preventive or improvement actions.

For the protection offered by the ISMS to be effective, the four steps described above should be continuously repeated in order to take into account changes, new risks as well as new objectives or business requirements of the organization.

Definitely, the importance of adopting an ISMS lies in the fact that information assets, risk management and related information security controls are managed and documented in a systematic manner where decisions are as much as possible integrated, scaled and updated reflecting any kind of objective and need of the organization. The successful consequences are achieving assurance about protection against threats and maintaining a framework that selects controls and improves their effectiveness. [6]

2.3 ISO/IEC 27001

ISO/IEC 27001, henceforth also just "27001", is a set of generic requirements that an ISMS must fulfill. Like other ISO/IEC standards about management systems, it follows a high-level structure that allows a more immediate application and a better ability to be integrated. The certification to 27001 is not mandatory: organizations can decide to adopt it as a reference of information security best practices but certainly obtaining an internationally recognized certification enhances their reputation and promotes the trust for customers. The 27001 is suitable for all types of organizations, regardless of their size or sector which means that, once the scope of the ISMS is defined, it can be directly applied in order integrate information security into the management process. The formulation of the requirements is consistent with the approach adopted by a management system,

namely implementing the Deming cycle[1]. Essentially, inside the document, requirements establish specifications in terms of context of the organization, leadership, planning, support, operation, performance evaluation and improvement. Although it is considered a requirements standard, a significant part is dedicated to a table of controls and objectives listed in the Annex A which represents a unique element among management systems due to its applicability in the information security field. This is the element connecting ISO/IEC 27001 and ISO/IEC 27002, where a brief control description is provided in the first standard and an exhaustive implementation guidance of it is given in the second one. In the next chapter dedicated to ISO/IEC 27002, the common history of the two standards will be better explained. [14, 4]

2.4 ISO/IEC 27002

ISO/IEC 27002, henceforth also just 27002, is a collection of generic information security controls approved as a *code of practice*. It provides a guidance about the implementation of each of these controls, specifying the purpose and the guidelines that should be pursued. Typically, the document is used by organizations to deploy effective measures of protection required to meet the objectives of ISO/IEC 27001 or to manage any risk. At the same time, it can be consulted during audit activity to perform a deeper analysis about what should be enforced. Since it is a guidance, 27002 cannot be certified. [14, 12]

2.4.1 History

The earliest version of what is known nowadays as ISO/IEC 27002 was published in 1992 by the Department of Trade and Industry (DTI) as a Code of Practice for Information Security Management. In 1995, it evolved into BS 7799-1, a national British Standard collecting a set of controls which are still recognizable in the current version of 27002. While in 1998 also information security requirements were formalized into a separate standard named BS 7799-2, BS 7799-1 was revised and it officially became ISO/IEC 17799 in 2000. Hence, it was promoted to international standard, like BS 7799-2 that was transformed into ISO/IEC 27001 in 2005. This implies that thereafter both next evolutions were handled by a global joint technical committee of ISO/IEC JTC 1 SC 27. In 2005, finally ISO/IEC 17799 was converted into ISO/IEC 27002 and the following years both controls and requirements standards were subject to consistent reviews due to the alignment they should have in terms of controls. Currently, the effective versions of ISO/IEC 27001 and ISO/IEC 27002 have been established in 2013 and 2022, respectively. [3]

[1] Also known as PDCA cycle (Plan–Do–Check–Act), *"the Deming cycle is an iterative design and management method used in business for the control and continuous improvement of processes and products"*.[19]

2.4.2 Evolution of its controls

As far as the structure of 27002 is concerned, the number of controls and their organization have evolved over the time. In the past, these reviews have not brought a real improvement: besides simply removing or adding controls without actually updating them, their organization within the document is not immediate and it is excessively layered, leading to its reduced use in favor of the simpler Annex A of 27001. For this reason, the objective of the last review aimed to overcome these limitations.

The result of this long and important review has been achieved recently: the new version has been published in February 2022 but when we started the thesis work, the development of the standard was in stage *Approval* as FDIS (Final Draft International Standard). Despite the effective version was still the ISO/IEC 27002:2013, we decided to adopt the most recent document, the FDIS, although it had not yet become effective as new replacing standard, because its publication would come shortly and the contents were already practically final. Since Annex A of ISO/IEC 27001:2013 is directly derived from and aligned with controls listed in 27002, the future review of 27001 will be affected by this innovation. [3, 11]

Year	2000	2005	2013	2022
N°controls	129	133	114	93

Table 2.1. Evolution of the number of controls of ISO/IEC 27002 over time

2.4.3 The new version

The last review of 27002, officially become effective as new standard version in February 2022, has lead to a significant reorganization where new controls where added, existing ones updated, aggregated or removed, and a new classification have been introduced. While the old version defined 14 security control clauses, 35 security control categories and overall 114 controls, the new one classifies 93 controls in 4 themes. In this way the structure of the document turns out to be easy to understand and identifying controls becomes easier. In order to simplify the future use of this different reorganization, two mapping tables has been appended within the Annex B of the new version: they help to properly identify the correspondence between old controls and new ones and vice versa.

Structure of the new document

The new design approach introduces the following key concepts and ideas:

- A theme is a categorization such that each defined control fits into a single theme
- An attribute is a piece of information describing a characteristic of a control based on a defined property

- The collection of controls is organized according to 4 themes. They have been classified into:
  - Organizational controls
  - People controls
  - Physical controls
  - Technical controls
- Each control has a set of associated attributes
- Controls can be associated with one another and grouped by these defined attributes

Consequently, the structure of a single control has been updated with respect to the old one containing *Control*, *Guidance* and *Other information*: the *Table of attributes* and the *Purpose* have been added by the new version. In this way each control is well defined and easily identifiable according to its theme classification and its attribute values. This structure supports the utilization of further specific guidelines or other frameworks and it allows to better locate any future update of the guidance content. [3, 11]

Table of attributes

The table of attributes permits to describe a control based on defined properties, that represent the values that each attribute can assume. The five attributes are the following:

- Control type: specifies if a control is Preventive or Detective or Corrective
- Information security properties: identifies if a control contributes to preserve Confidentiality, Integrity and Availability
- Cybersecurity concepts: identifies the five functions of the cybersecurity framework within the organization (Identify, Protect, Detect, Respond, Recover)
- Operational capabilities: are used to classify controls from the perspective of the practitioner
- Security domains: are used to classify controls from the perspective of information security domains, expertise, services and products (Governance_and_Ecosystem, Protection, Defence, Resilience)

A brief explanation of the meaning each attribute, how it should be used and the possible values it can assume are presented in Annex A of the document, together with a summarizing matrix of all controls and their assigned attribute values. [11]

2.5 ISO/IEC 27008

ISO/IEC 27008 is classified as a Technical Specification[2] deliverable. It provides a guidance on how to review and assess information security controls selected for meeting information security objectives and supporting information security risk management. This document is intended to be used for verifying the efficiency and effectiveness of implemented controls in order to confirm their suitability or to identify the need for changes. Typically this activities are carried out during audit, which means that the auditor has the responsibility to analyse the target of evaluation following the guidelines provided by ISO/IEC 27008.

Specifically, ISO/IEC 27008 defines:

- The assessment process for information security controls, including a preliminary gathering information phase, the definition of the audit scope, the review fieldwork and the analysis process.
- The review methods, including techniques used for examination, testing and validation, and sampling.
- The control assessment process, that specifies how to plan and perform the assessment of controls and how to analyse and report results.

A consistent section of the document is composed of the Annex A,B and C which provide further informative parts of the standard. As far as assessment of controls from the ISO/IEC 27002 is concerned, Annex B is intended to be used as a table of practice guide for technical security assessment. The current version of ISO/IEC 27008 deliverable dates back to 2019, which is why the controls that are listed for check in Annex B are identifiable in the 2013 version of ISO/IEC 27002. [7]

[2] A Technical Specification is a deliverable that is intended to be adopted for immediate use when published, but it could be a possible International Standard in the future. [9]

Chapter 3

Audit process

This chapter introduces the concept of audit through some basic definitions and typical classifications of the audit activity, intended in the wide sense of the term, which means that the following concepts are not restricted to information security management system only.

3.1 What is an audit?

As defined by the reference standard *ISO 19011 - Guidelines for auditing management systems* [5], an audit is a *"systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled"*. In this definition, it is highlighted how activities for audit purposes should be carried out according to a fixed prearranged plan (*systematic*), by entities separate from those audited (*independent*), and everything should be *documented*. Specifically, the conformity is determined with respect to a set of requirements used as a reference (*audit criteria*), which include for example policies, standards, legal, contractual and management system requirements. They usually come from different sources, such as regulations, international standards, industry practices and organizational policies.

The primary purpose of audit is the assessment of the system or organization subject to verification, which represents the auditee, where strengths and weaknesses are determined on the basis of evidence and facts found in an objective manner. Consequently, the auditor identifies what the auditee does and how, aiming to determine if adopted techniques and practices are in compliance with the organizational policies, requirements, processes, and related standards as well as laws and regulations. Finally, the ultimate action is communicating obtained results to who is responsible for the audited system, usually the top management, which then will provide for deciding appropriate measures.

Audit can be aimed at different areas, such as financial and administrative, which means that the activities are devoted to check the compliance with respect to legal and administrative requirements, respectively. Otherwise, in the scope of information security, we talk about information system security audit which determines the suitability of the protection applied on the information assets. [15]

3.1.1 Types of audits

Depending on the relationship between the auditor and the auditee, three types of audits can be identified:

- First-party audit: it is conducted by the organization itself. It aims at giving an assurance level about adopted processes, by evaluating requirements, policies and procedures that the organization forced itself and providing suggestions and possibilities for improvement. The auditor can be an employee or someone who serves on behalf of the organization itself.

- Second-party audit: it is conducted by an external entity which has an interest in the subject of audit, such as suppliers that want to check contract requirements fulfilment, but without certification purposes.

- Third-party audit: it is conducted by independent audit organization, such as certification bodies and governmental agencies, and it aims at ensuring compliance with respect to a specific standard in order to obtain a certification.

Since first party audits are performed by the organization itself, they are typically referred to as Internal audits, while second and third party ones are also known as External audits.

From the point of view of the purpose of the audit, audits can be classified as opinion audit, pre-evaluation audit and certification audit: the purpose of the first one is to obtain advice and recommendations, while the second and third ones aim to prepare and obtain a certification, respectively. [15]

3.2 Principles

Audit activities are based on a set of principles that auditors should adhere to. Their implementation is an advanced guarantee about effective and reliable outcomes resulting from auditing because, in this way, even auditors working independently from each another should obtain similar conclusions in similar circumstances, due to the fulfillment of the same principles.

Specifically, the audit process relies on the following seven principles: [5, 15]

- Integrity: in this context, it is intended as a set of rules of professional behavior, which are the basis for ethical, honest, and responsible work. It includes the ability of auditors to be impartial, uncorrupted, and fair during the judgment. For example, in order to assess the performances of auditors, a customer satisfaction questionnaire can be provided to the auditee when the audit is terminated.

- Fair Presentation: it is referred to the obligation to report audit findings and conclusions truthfully and accurately, preserving their objectivity even in the event of diverging opinions that arose during the audit.

- Due Professional Care: as defined in ISO 19011, it underlines the fact that *"Auditors should exercise due care in accordance with the importance of the task they perform and the confidence placed in them by the audit client and other interested parties"*. Basically, auditors should apply diligence and professional judgement, which means that they have to consider the presence of some factors that could affect their decisions.

- Confidentiality: it is a basic property that refers to the security of sensitive or confidential information. In this context, the auditor should use the information to which he is given access preserving its confidentiality through proper handling. Therefore, on one side reasonable measures should be adopted to ensure that personnel is not violating its confidentiality agreements when disclosing information to the auditor, on the other side the auditor should respect the principle also when the relationship with the auditee ends.

- Independence: it is an essential characteristic of the audit to ensure objective conclusions to be achieved. In principle, auditors should be independent from the auditee in order to preserve the impartiality. However, sometimes it may not be fully practicable, such as in case of internal audit in small organizations: anyway effort should be put in removing as much as possible bias and conflict of interest by verifying that conclusions are always legitimated by audit evidence.

- Evidence-based approach: it is the method that is based on the use of audit evidence considering samples of information that can be subject to verification and consequently are the prerequisite for reliable conclusions on the compliance with the audit criteria.

- Risk-based approach: it is the audit method that focuses differently on audit areas depending on the risks to which they are exposed. Therefore, distinct levels of effort and a variety of techniques should be adopted accordingly. This approach is maintained throughout the planning process: it means that it should support the risks management cycle and continuously reflect the related priorities defined by the organization.

3.3 Audit evidence

Definition and characteristics

As previously introduced, the term Evidence-based auditing underlines the importance of audit evidence as a prerequisite for reliable conclusions on the compliance with respect to the adopted criteria during the audit process.

Audit evidence can be defined as a relevant and reliable piece of information, whose properties are necessary for it to be considered appropriate. Relevant means that it can be effectively applied as input to assess conformity, while reliable refers to the fact that the information is perceived as a faithful with respect to what is should represent. By a way of example, it is clear that an organization chart or a function chart is a relevant evidence

for the verification of the segregation of duties, and it is also deemed to be reliable since it is documented and approved by the top management. If the level of assurance that is achieved with audit evidence is acceptable, then it can also be considered sufficient. The type and amount of required evidence are typically determined on the basis of the auditor's experience and evaluating the available resources, also in terms of time for conducting the audit.

3.3.1 Types of audit evidence

The reliability of the audit evidence depends on several factors and properties that characterize the information itself and how it is acquired. As far as provided reliability is concerned, audit evidence can be classified into seven categories where each one gives assurance of a certain level of reliability, as shown in figure 3.1.

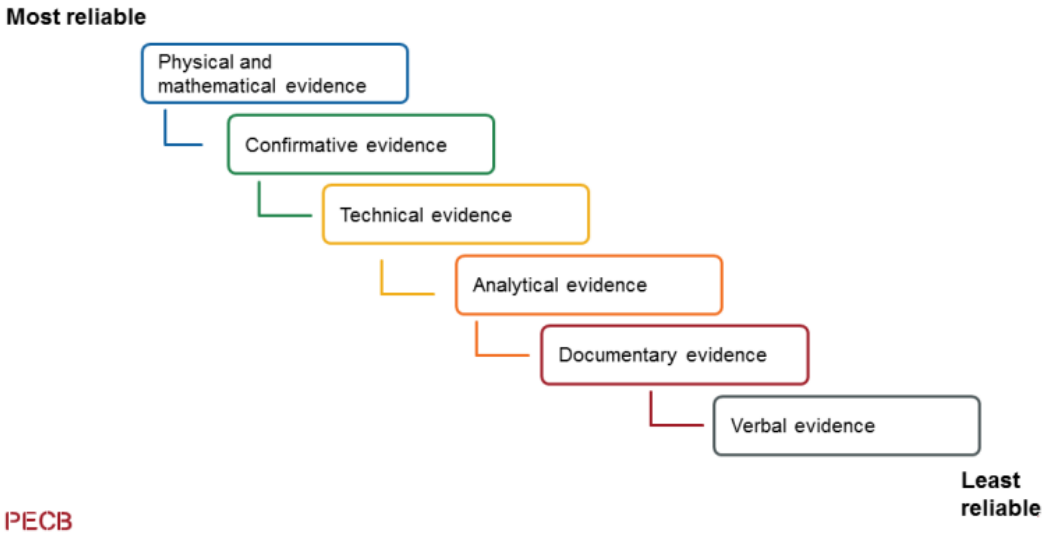

Figure 3.1. Reliability of audit evidence [15]

In principle, the classification is made such that the more objective the evidence is, the more reliable it is considered. Specifically, a brief description with straightforward information security examples of each type is given below-

1. Physical evidence is the most reliable type of evidence. Its physical existence is an inherent proof which is obtained through direct observation and inspection of tangible elements.
    - Examples: observation of fire protection devices, information labelling, physical entry controls
2. Mathematical evidence is based on the assurance given by the mathematical exactness of the calculation over certain documents or records.

- Example: number of training hours to validate the information security awareness (ISO/IEC 27002, Clause 6.3 Information security awareness, education and training [11])

3. Confirmative evidence derives by the confirmation provided by a third party regarding elements inspected during the audit. The conferred reliability is proportional to the confidence that the auditee gives to the third party moreover, the fact that the latter is independent from the first is discriminating factor.

   - Example: report from an external consultant about segregation of networks of information services, users and information system groups (ISO/IEC 27002, Clause 8.22 Segregation of networks [11])

4. Technical evidence arise from the analysis of technical test results and considerations.

   - Examples: logs collection, review firewall configuration rules to verify that only allowed network and services have allowed network traffic (ISO/IEC 27002, Clause 8.21 Security of network services [11])

5. Analytical evidence is obtained through statistical methods, and generally from the analysis of data to identify their tendencies and potential deviations.

   - Example: review of network access records to verify their correctness, like temporary rights that should be removed the expiration (ISO/IEC 27002, Clause 5.18 Access rights [11])

6. Documentary evidence is based on the analysis and verification of any form of documented information.

   - Examples: analysis of information security policies and topic-specific policies (ISO/IEC 27002, Clause 5.1 Policies for information security [11]), analysis of confidentiality or non-disclosure agreement clauses (ISO/IEC 27002, Clause 6.6 Confidentiality or non-disclosure agreement [11])

7. Verbal evidence is the most adopted and at the same time the least reliable type of evidence, since it is based to the verbal verification coming from interviews with the personnel responsible for the operations that are being audited. For this reason, additional evidence are necessarily required to support the verbal one.

   - Example: interview the top management to understand how information security responsibilities are defined and attributed (ISO/IEC 27002, Clause 5.2 Information security roles and responsibilities [11])

3.4 Audit procedures

The audit process is composed by a number of phases that contribute to implement a systematic approach. Typically, as a preliminary step, the initiation of the process includes

determining the audit feasibility, which means that audit objectives, scope and criteria must be established in order to define the schedule and planning activities accordingly.

As shown in figure 3.2, ISO 19011 standard defines seven steps of a typical process that aims to perform an audit by collecting information on the basis of which the audit conclusions are reached.

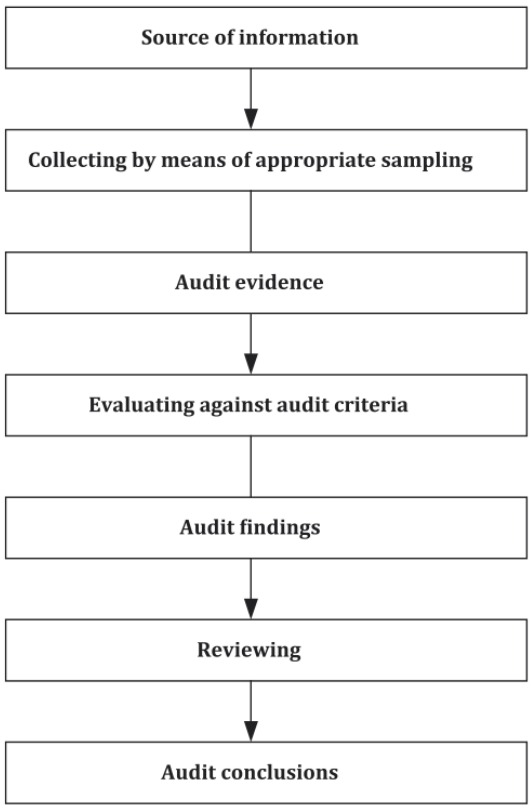

Figure 3.2. Process of collecting and verifying information [5]

The audit procedure consists in methods and steps that are followed by the auditor to collect reliable and relevant evidence. Since obtaining more evidence contributes to reach better conclusions, the auditor should also take into account to draw from several sources of information. The adopted strategy should be devoted to use different audit procedures depending on the type of evidence to be obtained and this can be achieved by means of methods such as interviews, observation of processes and activities, and review of documentation. Collecting information usually requires appropriate sampling: when analysing the 100 percent of the items is not feasible, the auditor must select a sample of items which are representative of the whole auditee. By a way of example, whenever backup systems are under evaluation, just different configurations of them are selected and analysed, not all devices that deploy them. In general, sampling is achieved through systematic or random selection.

In the evidence collection phase it is important to underline that this also includes the utilization of several analysis tools and techniques, as well as procedures, which may vary from one auditor to the other. In order to balance the possible variation deriving from that, it is generally required to adopt a specific, predefined combination of procedures. Practically, in the previous example context, it means that auditors can interview who is responsible for backups to know how they are performed and they can also review steps of the related documented procedure or observe a sample of backup being performed.

The common factor among different techniques of auditing remains the assurance to be achieved by the audit conclusions which must be as much objective as possible. The adoption of audit procedures contributes in this direction by reducing audit risk of being dis-aligned with others' conclusions. The decision between compliant and non-compliant evaluation is based on the experience of auditors, which is why having a guideline of procedures would reduce the subjectivity of the assessment. In this sense, a standard of audit procedures will overcome this limitation. The development strategy adopted in this thesis work relies on the concepts set out above. [16, 5]

3.5 Audit results

As previously shown in figure 3.2, after the collection phase, audit findings are determined through evaluation of audit evidence with respect to the prearranged audit criteria and they represent the determining factor in drawing the final audit conclusions. Specifically, audit findings should consider several aspects such as audit client's requirements, extent to which planned activities are realized and results achieved, and accuracy, sufficiency, and appropriateness of the evidence. The inherent subjectivity of the whole audit activity is introduced in this step where audit findings are generated from objective audit evidence submitted to the experience of the auditor.

Audit findings can be classified to indicate conformity and nonconformity [1]:

- conformity: it identifies the fulfillment of a requirement, intended as whatever prearranged requirement in the scope of the audit. Typically, it can be accompanied by observations and any recommendations in order to point out possible opportunities for improvements.

- nonconformity: it identifies the non-fulfillment of a requirement, further supported by audit findings. Depending on the extent of the risk exposure, they can be usually classified as:

  - Minor nonconformity: it partially fulfills the requirement but presenting a non-negligible risk or raising doubts about the real effectiveness of the management

[1] As noticed in ISO 19011 [5], *"Conformity or nonconformity with audit criteria related to statutory or regulatory requirements or other requirements, is sometimes referred to as compliance or non-compliance"*.

system. For example, if continual improvement of information management system is required and actually performed but it is not included in the documented policy, this represents a minor nonconformity.

- Major nonconformity: it represents the nonfulfillment of requirement which introduces an unacceptable level of risks. This type of nonconformity typically leads to a failure to obtain the auditee eligibility and consequently requires audit to be arranged again after solving major nonconformities. For example, if authentication mechanism is not enforced to every mobile communication device, this represents a major nonconformity.

In any case, both conformity and non-conformity records should be supported by appropriate audit evidence, description of the audit criteria against which conformity or non-conformity is shown and the respective declaration.

Ultimately, auditors prepare an audit report that documents the activities performed according to the planning and underlines audit conclusions, including whatever concerns auditing such as its scope, objectives, criteria, findings and evidence, and any additional detail that makes the report clear, accurate and complete. [5, 17]

Chapter 4

Design of audit procedures

In this chapter the design process of developed procedures will be analysed. Initially the definition of the problem that the thesis work is intended to solve will be explained and then the approach with which useful documentation has been analysed will be introduced, especially a well-known example of standardized audit procedures taken as a reference both in design and implementation phases. According to the previous considerations, the design of the audit procedures will be presented.

4.1 Overview of the current scenario

4.1.1 Context of application

The auditing of an Information Security Management System constitutes the reference scenario where the thesis work is intended to be applied. From the 27000 family point of view, it materializes in auditing organizations' management systems against ISO/IEC 27001 standard and against its Annex A, that basically means ISO/IEC 27002, for the related controls implementation. In this context, audit procedures represent a recognized set of methods and steps of performing evidence collection that guide the auditor in the evaluation of organizations' information security.

4.1.2 Problem definition

Audit consists of several systematic activities in which the role and the experience of the auditor introduce a remarkable degree of subjectivity and consequently the audit findings are strongly affected by it. In the context of application previously introduced, the guidance of ISO/IEC 27008 represents a useful reference document which can be consulted by auditors for the assessment of information security controls specified in ISO/IEC 27002. In principle, the presence of a standard that establishes how to review the implementation of the controls introduces a high degree of homogeneity in the final results. Nevertheless, the current version of ISO/IEC 27008 does not describe detailed procedures for each information security control to be verified, which means that evaluations performed by

distinct auditors can vary from each other and the accuracy of the analysis can be affected by some subjective factors.

In particular, in the compliance verification process of a single information security control, it is not rigorously defined what needs to be inspected for proving a specific property and giving a certain level of assurance: the kind of documentation, process, configuration, or whatever concerns evidence collection is decided and consequently evaluated at the discretion of the auditor. This freedom of decision leads to a lack of comparability between results obtained from different audit activities because there is no standard procedure that defines how and by what means a certain audit conclusion should be drawn. The major risk is constituted by the assertions of conformity that derive from wrong assumptions, such as implemented measures of protection which are not actually effective. This risks exposing the organization's assets to threats that have not been considered or that are perceived to be adequately handled.

These are the main reasons that justify the need for utilization of audit procedures to be followed by auditors to ensure a rigorous evaluation of compliance of information security controls' implementation.

4.2 Goal of the proposed solution

The thesis work has set itself the objective of realizing audit procedures designed to be adopted throughout audit activity of organizations aiming to be ISO/IEC 27001 compliant. The procedures are intended to be applied for verifying the information security controls deployed to face and mitigate information security management system's risks and, consequently, ISO/IEC 27002 standard document has been taken as a reference for the entire procedures' development process. The proposed solution aims to guide the auditors to achieve audit objectives in a more comparable and objective manner through a well-defined series of steps that include which evidence collection strategies should be deployed and the reason for the procedure itself. The ultimate purpose is trying to standardize the audit process and reduce its subjectivity. [16]

4.3 Preliminary work

4.3.1 Workplan and adopted strategy

Before understanding what an audit procedure should consist of and how it can be structured, first of all the thesis work has been planned to start with an initial cognitive activity. This was aimed to get familiar with the ISO/IEC 27002 document, its content and utilization context, and to gain knowledge about auditing and audit procedure objectives.

Specifically, an important standard has been considered as a useful hint: PCI DSS, which stands for Payment Card Industry Data Security Standard, is a widely deployed standard for protecting payment cardholder data, whether they are used in payment

transaction or as a backup or in a chargeback process[1]. It is the worldwide reference that all companies that process, store, or transmit credit card information should comply with in order to ensure a secure environment for payment cardholder data. In the context of this thesis work, the adopted strategy for learning how to write down a audit procedure has taken advantage of the well-known PCI DSS because it provides detailed audit procedures to be used during the standard compliance assessment process. In the next subsection the information gathered from the analysis of this standard will be introduced, focusing on it as a useful starting point for devising the structure and the language of employed audit procedure in ISO/IEC 27002 context.

The workload has been organized as follows:

1. Analysis of PCI DSS standard as reference for audit procedures, and ISO/IEC 27002 FDIS document as new classification of information security controls
2. Definition of the structure of a test procedure
3. Draft version of audit procedures
4. Revision and final version of audit procedures

4.3.2 PCI DSS as a reference

PCI DSS standard is derived from a common need to overcome the problem of security breaches that MasterCard and Visa had to face: they merged their workaround programs to unify the industry and later major card schemes like American Express, Diners Club, Discover Card and JCB were incorporated by the expanded PCI SSC as an entity. Recently also China Union Pay has joined them. The need of uniformity comes from the worldwide importance of the card payments and relative environment protection: essentially, the standard is applied to all merchants and service providers that store, process or transmit cardholder data so over the years it has become the de facto standard. With respect to ISO/IEC 27001 that defines requirements and a list of controls, PCI DSS is more prescriptive since it additionally specifies testing procedures associated to each requirement, to be rigorously observed for the compliance validation performed by the auditor. [18]

As previuosly introduced, the document is as a standard that provides a baseline composed of technical and operational requirements designed for the protection of cardholder account data combined together with corresponding testing procedures. This joined design permits to use PCI DSS standard both for requirements implementation and as part of the standard compliance assessment, binding two independent activities to the same reference document. From the point of view of auditing PCI DSS compliant systems, this strategy greatly simplifies the verification activity and encourages the homogeneity of its

[1] *"The chargeback process encompasses all the steps that take place between a cardholder contacting the issuing bank to dispute a charge, and the resolution of that dispute. Multiple parties, including issuers, acquirers, merchants, vendors, and card networks may be involved in this process"*. [1]

execution process because the connection between requirement and testing procedure is straightforward.

As far as testing procedures of PCI DSS are concerned, they have been analysed in order to observe which kind of evidence supports certain verification statements and, consequently, they have been used as a starting point for devising the structure and the language of audit procedures in the context of information security controls. Indicatively, the inferred pattern correlates macro topics of requirements with certain types of testing techniques, as shown in the table 4.1 where some explanatory examples have been reported.

High-level identifier	**Requirement clause**	**Testing methods**
1	Network traffic protection, like firewall installation and rules	The evaluation includes examination of configuration settings and interview to the interested personnel
3	Stored data protection	The verification includes analysis of the documentation, inspection of physical device, relative configuration settings and interview to the interested personnel
4	Mechanisms of protection of transmitted, stored and processed data	The processes that regulate these mechanisms are observed to verify their correctness and also their relative documentation, in addiction to interviews to personnel
5	Risk management and maintenance	The evaluation is performed through examination of the documentation and interview
6	Common best practices knowledge and utilization	The evaluation of the knowledge is typically performed analysing documentation, interviewing and reviewing records to check how personnel is trained and how common practices are applied in processes or procedures.
12	Acknowledged policies, formal processes and procedures that should be established in a written form and agreed by the responsible personnel	The evaluation is performed through examination of the documentation and interview of the interested personnel, when practicable or applicable

Table 4.1. Application pattern of testing methods in PCI DSS standard

In addition, the analysis of testing procedures has highlighted the level of detail they should have in order to be precise, sufficient and effective. In this case, we have taken as a reference a widely deployed standard which has a restricted field of application in

protecting payment cardholder data, so this is the reason why such procedures are legitimated to be very precise and accurately detailed. On the contrary, the terminology of ISO/IEC 27002's information security controls is definitely generic: in the definition of the single procedure it will be necessary to maintain a level of abstraction such as to allow its application to all types of organizations, different in terms of sector and size.

In the light of these considerations, an attempt was made to find a similarity between requirements of PCI DSS and controls clauses of ISO/IEC 27002. In such manner, during the following development of the audit procedures, we employed PCI DSS testing procedures as a benchmark to identify possible improvement. [13]

4.4 Structure of a test procedure

Following the methodology used by PCI DSS consolidated procedures, it has been decided to endorse a similar idea for the structure of realized audit procedure: the employed approach systematically aims to submit the control verification process to multiple audit procedures of different types. This implies that for each information security control a specific, pre-defined combination of testing procedures has been assigned. To this purpose, the following four testing methods illustrated in 4.1 have been established, and the structure of the test procedure has been defined accordingly, as shown in figure 4.2.

Figure 4.1. Combination of four testing methods

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation

Figure 4.2. Design of the audit procedure structure

The labels characterizing the chosen structure are intuitively understandable:

- **ID**: unique control identifier in ISO/IEC 27002:2022 document
- **Control**: statement describing what the control is, as defined in ISO/IEC 27002:2022 document

- **Testing Procedure**: title describing the testing procedure scope of interest
- **Interview**: testing method based on verbal interview, explained in 4.4.1
- **Document**: testing method based on the analysis of any written form of documents, explained in 4.4.2
- **Configuration**: testing method based on the inspection of configuration settings, explained in 4.4.3
- **Observation**: testing method based on the observation of a process or of its outputs, explained in 4.4.4

4.4.1 Interview

The interview is the most widely used testing method, both in this thesis work and in general by auditors. It consists in a series of pre-defined verbal or written questions to which auditee's employers are subjected. This form of audit procedure turns out to be easier to implement because it requires less time and effort on the auditor side, it allows to collect information of different entities but relating to the same topic simultaneously, and it is the most flexible. By a way of example, as far as surveillance system is concerned, the auditor can gather information about what surveillance measures are present, how they are employed for monitoring, how frequently and by who, by interviewing the responsible personnel.

Since interview is inherently based on verbal evidence which is the least reliable, according to the classification presented in 3.3.1, this implies the need of providing additional types of evidence that supports verbal ones. This is the reason why, during this thesis work, testing method based on interview has always been integrated with other methods.

Types of interviews

Interviews can be conducted through several approaches, aiming to obtain an adequate pre-established level of coverage of all target items. Thus, interviews can be:

- General vs Detailed: it depends on what the interview aims to validate, leading to a different level of detail in gathering information process. For example, if the target is the general design of human resources management process or it is a recovery plan of a incident management process, auditor will conduct a general or detailed interview, respectively.
- Individual vs Group: it is intended for a single person or a group of individuals. Group interviews are less frequent and they are usually performed when is necessary to analyse the interactions between members, so typically individual interviews are more common.

Results, conclusions and any type of information deriving from interviews of any form should be appropriately recorded. [16]

4.4.2 Documentation

The method based on the documentation consists of the review of documents like policies and procedures and formally recorded information. It is performed as a preliminary step of effectiveness of control implementation, so typically first documented process existence is checked through documentation analysis and then its effectiveness and compliance will be validated, producing documentary evidence (following the classification in 3.3.1). From the point of view of the results, documented information review is appropriate for understanding and evaluating the management system functioning and design, and related controls from a broader perspective. In the context of developed audit procedures, documentation method has been adopted whenever possible to analyse policies or any well-formed procedure or process, considering the feasibility of the method according to the kind of information that usually are documented or not.

The validation of documented information is performed by evaluating:

- the correspondence of its content with respect to the represented clause
- its format conformity
- the relative procedure for the management of the documented information

[15]

4.4.3 Configuration

This audit method consists in the analysis of configurations, intended as configuration settings of the system or application under evaluation. It is adopted to validate the effectiveness of a technical control in place, for this reason it can be applied to systems where configuration settings are meaningful for the fulfillment of the control purpose. This implies that this method is typically targeted to any kind of device, hardware or software component, or in general any IT system where the configuration values are relevant and must be verified by the auditor. Consequently, the analysis of configurations produces technical evidence, which has a medium level of reliability according to the classification in 3.3.1. The auditor usually does not verify the configurations autonomously but asks a system administrator to show them or, if particularly large or difficult to analyze, to export them. In the context of this thesis work, it has been mostly used in technological controls of ISO/IEC 27002. [16]

4.4.4 Observation

This audit method is performed through direct observation of the phenomenon subject to the audit activity. Typically, it can include physical inspections, records examinations, and in general whatever observation aimed at verifying processes, procedures as well as the implementation of information security best practices, such as firewall updates. Since it produces physical evidence, the best in terms of reliability, the observation is certainly the most reliable form of audit method, because it adopts a broader perspective given by the fact that a procedure or process is considered in its entirety.

Depending on the depth of the auditor analysis, this method can be performed through general or detailed observation. Respectively, the former aims to verify just the existence of a process and its implementation, and the latter examines in detail the functioning and continuity of a process. For example, the visit of the data-processing center and the observation of a system backup test are illustrative of the different level of analysis detail.[16]

4.5 Strategy of development

4.5.1 Main principles

According to the previous considerations about procedures' characteristics in ISO/IEC 27002 context, the adopted strategy has deployed the following principles which have influenced the used language and the level of detail of the developed audit procedures:

- General attitude: the language, as well as the level of detail used in writing the procedures, has been maintained as much general as possible, according to the fact that audit procedures should be applicable to organizations of any type, sector and size, reflecting the nature of ISO/IEC 27002. Nevertheless, they had to be precise in order to adequately identify the scope of interest of the control evaluation target and define how to assess its compliance.

- Relevance: even if guidance provided by ISO/IEC 27002 document has been used as a baseline during the definition of a testing procedure, not all aspects presented in the guidance of each control have been deeply verified. The main reason is that the relevance that some topics have in practical audit activities has been considered to decide whether to include them or not, leading to develop procedures just for the main aspects.

- Removal of repetitions: since some controls' guidance considers overlapped features to be verified, redundant aspects introduced by different controls were included only in the most significant one in order to avoid repetitions during the verification activity performed by the auditor.

4.5.2 Combination strategy

The combination strategy is strictly bound to the nature of the control itself, but generally, for each testing procedure, the essential ultimate purpose has been intended to combine at least two testing methods among the four defined. As already mentioned in the audit introduction chapter, the main reason has been that this kind of combination guarantees a higher level of assurance about the obtained results. Furthermore, each method provides a different level of reliability depending on the type of audit evidence it is based on. This implies that each test procedure has always two or more testing methods supporting each other and validating the audit conclusions. Practically, this translates into almost always present verbal assertions which are subsequently confirmed or denied by more

reliable evidence. Nevertheless, it should be mentioned that not all testing methods are applicable to all controls, due to the fact that some aspects are not inclined to certain verification techniques. This derives from the natural tendency of each control topic, and this can be especially highlighted analysing them at the level of the four themes defined in ISO/IEC 27002. [16]

Chapter 5

Implementation of audit procedures

Following the controls grouping scheme used by the ISO/IEC 27002 document, in this chapter the developed audit procedures will be presented through an analysis of controls' purposes, required protection measures and related activities to be performed by the auditor for verifying their implementation. The entire work and the following discussion are fully based on the FDIS version of ISO/IEC 27002 document [11].

5.1 Organizational controls

5.1.1 Introduction

Organizational controls are presented in Clause 5 of ISO/IEC 27002 document, collecting overall 37 controls which most of the time concern management aspects. The innovative introduction of attributes describing each control permits to group them creating different views. In this manner, it possible to identify more precisely the which are the common purposes of organizational controls and which are their operational capabilities.

Through a simple overview of the *Control type* attribute, it is clear that organizational controls are mostly preventive, and those corrective ones represent more than half of all corrective controls among all categories, thus it can be deduced that information security prevention and correction activities and relative responsibility largely depend on organizational controls. Furthermore, this attribute, together with the values of *Cybersecurity concepts*, directs the audit procedure purpose by suggesting which kind of evidence is needed for properly validating the implementation. Since organizational controls are preventive and should Identify and Protect information security assets, supporting evidence should be devoted to guarantee inherent protection.

As far as *Operational capabilities* is concerned, this attribute allow to further identify six groups of topics among all organizational controls, including:

- Governance controls: about 5.1 to 5.8

- Assets, Information protection and Identity and access management: about 5.9 to 5.18
- Supplier relationship controls: about 5.19 to 5.23
- Events management controls: about 5.24 to 5.28
- Continuity: about 5.29 to 5.30
- Legal and compliance: about 5.29 to 5.37

While writing interviews' procedure, it has been decided to maintain language and terminology as general as possible due to the fact that each organization can have different roles that are responsible for certain areas of competences can be distributed differently depending on the type and size of the organization. Next subsections will present the developed procedures.

5.1.2 Audit procedures

5.1 Policies for information security

- Control: *"Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur."* [11]

This control regards information security policies and its management at the highest level within the organization: the related procedures have been designed to verify their communication, approval, maintenance, acknowledgement and awareness. Specifically, almost every testing procedure resorts to interview, due to the fact that for management requirements the auditor takes advantage of the interaction with the top management responsible. The purpose during the interview is evaluating how communication, approval, maintenance, acknowledgement and awareness are implemented. As concerns topic-specific policies, at this high level of control the procedure does not provide for inspection of the content of these policies since they will be analysed directly in the related control, but just its exhaustive coverage is checked. In the case of communication, acknowledgement and awareness, they can not be verified through documentation analysis as approval and maintenance do, for this reason the observation is a useful method for a adequate verification.

5.2 Information security roles and responsibilities

- Control: *"Information security roles and responsibilities should be defined and allocated according to the organization needs."* [11]

In this control a single audit procedure uses three methods to verify the adequate definition of roles and responsibilities. In this context, the most relevant evidence derives from the

analysis of the so-called organization charts[1] and function charts: they represent two important instruments for a general overview about the allocation of roles and related responsibilities, and for verifying the related job description. During the assessment, the auditor must verify the clear definition of information security responsibilities through the analysis of charts, regarding:

- protection of information and associate assets
- carrying out information security processes
- information security risk management activities
- all personnel's involvement in information security

5.3 Segregation of duties

- Control: *"Conflicting duties and areas of responsibility should be segregated."* [11]

This control is strictly related to the previous one, but with a more precise purpose: requiring that conflicting duties and responsibilities are segregated when necessary. This requirement aims to reduce the risk of information security controls being bypassed. In developed audit procedures, conflicting duties and activities requiring segregation are requested to be identifiable by means of organization charts and function charts, respectively, while through the interview the auditor's purpose is verifying duties segregation for what concerns the main activities like, for example, system administrators and developers.

5.4 Management responsibilities

- Control: *"Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization."* [11]

In order to verify that the management understands their role in information security, the audit procedures have adopted mainly the interview method because the awareness of responsibilities is something that is difficult to prove with other means. In this context, the auditor's ability should be focused on the analysis of how the management personnel ensures:

- adequate distribution of information security policies
- adequate means of communication of information security role and responsibilities
- conformity to information security considerations in contracts

[1] *"Organization chart is a graphic representation of the structure of an organization showing the relationships of the positions or jobs within it."* (Powered by Oxford Languages)

- the presence of a confidential channel for reporting violations on information security topics, additionally supported by observation method of the reported violations
- adequate resources allocation for information security activities, additionally supported by observation method of the plans and budgets for information security

5.5 Contact with authorities & 5.6 Contact with special interest groups

- Control 5.5: *The organization should establish and maintain contact with relevant authorities."* [11]
- Control 5.6: *The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations."* [11]

These two controls highlight the need to ensure an appropriate flow of information with the two relative entities. Basically, the approach of auditing is focused on the identification of relevant authorities and special interest groups, respectively. This is achieved by means of interviews and examination of the list of contacts practically used to get in touch with these entities and the verification of a sample of related communications.

5.7 Threat intelligence

- Control: *"Information relating to information security threats should be collected and analysed to produce threat intelligence."* [11]

This control is one of the new controls added in the latest version of ISO/IEC 27002: it has been introduced to provide ongoing awareness of the threat environment by collecting and analysing information about existing or emerging threats. For this reason the two developed audit procedures are focused on identification of relevant, insightful,contextual and actionable sources of threat intelligence[2] information and analysis of how they are integrated into the organization security process, respectively. In order to verify them, interview and observation methods have been deployed.

5.8 Information security in project management

- Control: *"Information security should be integrated into project management."* [11]

The integration of information security in the project management is one of the most relevant requirements from a prevention point of view. This control refers to information security requirements intended for all types of projects, not only Information and Communication Technology ones. Basically, what should be verified regards risks and requirements: in order for information security to be effectively addressed throughout the

[2]The term *Threat Intelligence* refers to the knowledge based on the collection of useful information to identify and understand possible security threats.

project life cycle, the audit procedures have been developed through interview and observation mechanisms. The full detailed version of the procedures can be found in Annex A.

5.9 Inventory of information and other associated assets

- Control: *"An inventory of information and other associated assets, including owners, should be developed and maintained."* [11]

This control requires a systematic identification and appropriate ownership assignment of information and other associated assets, therefore the auditor's purpose is aimed to assess inventories and ownership, especially in proportion to their importance in terms of information security. As regards inventory, the developed procedures have been interested in verifying its coverage, accuracy and update processes, through reviews of all inventories. As regards ownership, the single procedure employs interview to assets owners and observation of their formally accepted responsibilities in order to perform the asset management process.

5.10 Acceptable use of information and other associated assets

- Control: *"Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented."* [11]

This control aims to ensure appropriate protection, utilization and handling of information and other associated assets through the verification of the establishment of acceptable rules for their utilization. In this context, a topic-specific policy is defined and properly verified in its content suitability, through the analysis of the documentation that regulate the acceptable use of assets. The audit procedures have been defined also for assessing acceptable use procedures and third-party assets consideration.

5.11 Return of assets

- Control: *"Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement."* [11]

This control is focused on assets return management in case of change or termination of ownership. The developed audit procedures verify this process as regards knowledge return, prevention of unauthorized copies and returned assets, especially of certain critical equipment. From a physical point of view, what concerns organization's equipment return has been considered in audit procedures of the control 7.14. From a technical point of view, information deletion is strictly correlated to control 8.10 where all technical aspects are properly verified, while in this context only the procedures relating to the deletion of information when returning the assets are evaluated. The full detailed version of the procedures can be found in Annex A.

5.12 Classification of information & 5.13 Labelling of information

- Control: *"Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements."* [11]

- Control: *"An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization."* [11]

An adequate classification of information has an important relevance in the effectiveness of related protection measures: in this context, a topic-specific policy is defined and properly verified in its content suitability, through the analysis of the documentation that should establish the scheme for the classification including confidentiality, integrity and availability requirements and resulting impacts. In addiction, the alignment of this scheme with access control policy and business requirements represent another verification point. The developed audit procedures for clause 5.12 involve checks regarding consistency, review of the scheme and interoperability between different schemes. Consequently, the labelling of information (clause 5.13) is useful to facilitate its identification and support its automation processing, by reflecting the established classification scheme. As concerns the auditing, the observation method has been adopted to verify certain properties of classification labels and metadata, while the interview identifies how and when labels and metadata are applied. The full detailed version of the procedures can be found in Annex A.

5.14 Information transfer

- Control: *"Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties."* [11]

For information transfer, a topic-specific policy is defined and properly verified in its content suitability, through the analysis of the documentation. Following the control guidance structure, in addition to general information, three types of information transfer have been considered so three audit procedures have been developed accordingly: electronic and physical information transfer agreements are verified through the analysis of documented rules and procedures, and through the review a sample of them, while verbal information transfer awareness is subject to interview and review of verbal transfer security awareness initiatives records. The full detailed version of the procedures can be found in Annex A.

5.15 Access control

- Control: *"Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements."* [11]

Access control is a fundamental requirement for effective protection of information security, thus a topic-specific policy is defined and properly verified in its content suitability through the analysis of the documentation with a detailed checklist that suggests the link with other controls of ISO/IEC 27002. The other two developed audit procedures have been focused on access control rules and models, respectively: some points of control to be considered have been specified in the analysis of the access control rules, while the interview method has been aimed to retrieve the adopted access control models. In addition both for rules and models, consistency checks have been performed through configuration reviews. This is one of the few organizational controls in which the configuration method has been applicable and consequently adopted. The full detailed version of the procedures can be found in Annex A.

5.16 Identity management

- Control: *"The full life cycle of identities should be managed."* [11]

The processes involved in identity management represent an important preamble for proper authentication management, access control and access right. This control auditing manages unique and shared identities, and non-human entities through interviews and observation of the approval process. In the case of unique identity, the analysis of databases configuration is also applicable. Furthermore, audit procedures for identity disabling and identities information change have been adequately developed.

5.17 Authentication information

- Control: *"Allocation and management of authentication information should be controlled by a management process, including advising personnel of appropriate handling of authentication information."* [11]

Authentication information allocation and management are a crucial requirement, so respective auditing must be detailed in verifying every essential aspect that could open to potential risk exposure: this is why each audit procedure analyses a single property of a specific authentication information, which in this case regards password utilization. For this purpose, configuration method fits well for inspecting passwords settings. Notice that this is one of the few organizational controls in which the configuration method has been applicable and widely adopted. As regards other themes, the identity verification process and the reception of authentication information have been subject to audit procedures. The full detailed version of the procedures can be found in Annex A.

5.18 Access rights

- Control: *"Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control."* [11]

Access rights management is an essential requirement that is established according to access control policy and business requirements. The auditor aims to verify how the

owner of information grants access rights and how access rights are removed, modified, temporary granted and periodically reviewed: the observation methods permits to analyse records about each type of action to check they are performed correctly and timely. The full detailed version of the procedures can be found in Annex A.

5.19 Information security in supplier relationships

- Control: *"Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services."* [11]

The supplier relationships introduce another level of security risk that is not directly dependent from the organization itself. From the organization point of view, protection measures should be adopted to address potential risks associated with supplied products or services, so in this context the audit procedures have been developed to verify that the organization has implemented appropriate controls, risks assessment, non-conformance mitigation and secure termination of supplier relationship through interview and observation of evidence that supports the purpose of the procedure. The auditor has to analyse how suppliers are chosen and if the impact in terms of confidentiality, integrity and availability is properly evaluated. Furthermore, a topic-specific policy on supplier relationships is defined and properly verified in its content suitability.

5.20 Addressing information security within supplier agreements & 5.21 Managing information security in the ICT supply chain

- Control: *"Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship."* [11]
- Control: *"Processes and procedures should be defined and implemented to manage information security risks associated with the ICT products and services supply chain."* [11]

The clause 5.20 implies that information security requirements are included in suppliers agreements and consequently the related audit procedures have been developed to verify the content of these agreements and the fact that they are properly maintained in a register. This can be considered as a complementary part of the clause 5.21 because the common purpose is addressing information security risks associated with suppliers. In the context of 5.21 auditing, the developed audit procedures are focused on verifying the following activities through interview and review of supplier agreements:

- the propagation of security requirements to sub-contracted parts of the supplied ICT service
- proper critical components management
- how supplied components are verified to be genuine and unaltered
- how ICT supply chain risk management is implemented

The full detailed version of the procedures of clause 5.20 can be found in Annex A.

5.22 Monitoring, review and change management of supplier services

- Control: *"The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery."* [11]

This control regards the implementation of all activities of monitoring, reviewing, evaluating and managing change involving supplier services, which contribute to the previous controls' purpose. In this context, the audit procedures are aimed to verify the monitoring of performance and changes of supplied service, and the presence of an exchange of relevant security information between the organization and supplier through proper analysis of recorded monitoring activities and service reports, respectively.

5.23 Information security for use of cloud services

- Control: *"Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements."* [11]

The frequent adoption of cloud services requires a policy that complies with the organization's information security requirements: a topic-specific policy on the use of cloud services is defined and properly verified in its content suitability through the analysis of documentation. The audit procedures have been developed in order to analyse the criteria used to select the cloud providers and to evaluate the content of the agreements.

5.24 Information security incident management planning and preparation

- Control: *"The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities."* [11]

The implementation of this control ensures the presence of a quick and effective response to information security incidents. For this purpose, the organization should establish an incident management plan that includes all relevant aspects, as verified through the analysis of the documentation in first developed procedure. Then, incident management procedures and incident reporting procedures are evaluated by observing a sample of incident to verify they are applied according to the related documentation.

5.25 Assessment and decision on information security events & 5.26 Response to information security incidents & 5.27 Learning from information security incidents

- Control: *"The organization should assess information security events and decide if they are to be categorized as information security incidents."* [11]

- Control: *"Information security incidents should be responded to in accordance with the documented procedures."* [11]

- Control: *"Knowledge gained from information security incidents should be used to strengthen and improve the information security controls."* [11]

These three controls contribute to the same purpose of correctly identifying events that can be classified as incidents and responding in relation to the importance and impact conferred to such events. This abilities can be effectively improved using knowledge resulting from previous information security incidents. The audit procedures have been developed to verify:

- the categorization and prioritization scheme
- the documented incident response procedures
- procedures to gain information about the incident
- how incident management improvement

Except for incident response procedures which are documented, in all audit procedures interview and observation of a sample have been adopted as audit methods: as in the previous controls, the latter is typically intended to be a supporting mean for confirming that what has been declared during the interview is consistent with what has been done. The full detailed version of the procedures can be found in Annex A.

5.28 Collection of evidence

- Control: *"The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events."* [11]

In this control, evidence is intended for information security incidents support and it is required to be properly managed and maintained in order to be relevant and useful for the purposes of disciplinary and legal actions. The developed audit procedures aims to evaluate the evidence management procedures, which are usually documented, and the collected evidence quality, especially proving its integrity.

5.29 Information security during disruption & 5.30 ICT readiness for business continuity

- Control: *"The organization should plan how to maintain information security at an appropriate level during disruption."* [11]
- Control: *"ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements."* [11]

These two controls contribute to the same purpose of guaranteeing continuity during disruption: in clause 5.29, for information and associated assets security, this is achieved by adapting controls in place and by implementing compensating controls. Consequently, the two corresponding audit procedures have been developed to verify through interview and

documentation methods the effectiveness of such protection and responding measures. In 5.30, the business continuity must be preserved, so as far as information security properties are concerned, it regards only availability of the organization's information and associated assets. For this purpose, ICT continuity requirements, continuity plans and organizational plan to face disruption have been evaluated through testing procedures that always adopt interviews and documentation analysis. In addiction, continuity plans testing reports are reviewed to verify their exhaustiveness.

5.31 Legislation, regulations and statutory and contractual requirements

- Control: *"Legislation, regulations and statutory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date."* [11]

This control regards the compliance with external requirements and foreign countries. External requirements refers to any legislation, regulations and statutory and contractual requirements that is not strictly related to information security but is relevant to it. Those requirements must be taken into consideration within policies and procedures as well as in the related implementation. This verification is properly handled in the first audit procedure, while the second one aims to check how compliance with foreign countries requirements is addressed.

5.32 Intellectual property rights

- Control: *"The organization should implement appropriate procedures to protect intellectual property rights."* [11]

For intellectual property rights protection, a topic-specific policy is defined and properly verified in its content suitability, through the analysis of the documentation. The second developed audit procedure aims to analyse documented procedures defined to guarantee conformance in using software and products covered by intellectual property rights: this is further supported by evidence of ownership of a sample of software licences obtained through the observation method.

5.33 Protection of records

- Control: *"The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements."* [11]

This control regards records management both for information protection purpose and for conformance with external requirements. Available guidance is properly analysed during auditing to verify the inclusion of record and related retention schedules, while a sample of records is observed to verify its consistency with the documented information. The second audit procedure evaluates safeguards in place in order to protect storage and handling records through interview and documentation methods.

5.34 Privacy and protection of PII

- Control: *"Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release."* [11]

For privacy and protection of Personally Identifiable Information (PII), a topic-specific policy is defined and properly verified in its content suitability, through the analysis of the documentation. Then, procedures for its preservation and protection are evaluated in the developed audit procedure taking into consideration the implementation of controls mandated by applicable legislation.

5.35 Independent review of information security

- Control: *"The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur."* [11]

This control highlights the need of performing an independent internal review of information security and its implementation, generating reports that are subject to analysis by the auditor. In particular, the first audit procedure aims to verify that independent reviews are periodically performed by competent individuals independent of the area under review, while the second and the third ones regard additional reviews that should be managed when significant changes occur and the corrective actions management, respectively.

5.36 Conformance with policies, rules and standards for information security

- Control: *"Conformance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed."* [11]

This control ensures the conformity of information security implementation with respect to information security policy, topic-specific policies, rules and standards. This is achieved by the organization through reviews of conformance, and non-conformance management, which correspond to what the audit procedures verify through interview and observation method.

5.37 Documented operating procedures

- Control: *"Operating procedures for information processing facilities should be documented and made available to personnel who need them."* [11]

This control establishes that operating procedures are necessarily documented in order to guarantee secure operations. The range of activities that requires documented procedures are evaluated by the first developed audit procedure, while the second one regards the review and update to which operating procedures are subject.

5.1.3 Considerations

The presented organizational controls cover many different themes and aspects which have a fundamental preventive purpose for most of the time, as already said in the introduction. A general overview of developed organizational audit procedures highlights some common recurring patterns as regards:

- Topic-specific policies: they have always been analysed through interview and documentation analysis, so the corresponding audit procedure has resorted to verbal and documented evidence, by verifying that the policy is established and communicated to all relevant interested parties and that it contains and properly regulates the fundamental related requirements.
- Procedures and processes: in the audit procedures that analyse procedures or processes adopted internally, in addition to the interview, sometimes documentary review and sometimes observation have been used: this choice was dictated purely by pragmatic and realistic considerations since it depends on whether procedures and processes have been formalized or not.
- Specific aspects: the guidance of ISO/IEC 27002 reference document is well-detailed and many times is specified that some aspects could be not applicable, especially in small size organization. In those cases, the strategy adopted in writing the audit procedures has tried to avoid this possibility by including the essential features to be assessed.
- References to additional ISO standards: in several controls, such as the ones relating to cloud services, information security incident management, or protection of PII, further guidance can be found in other ISO standards, thus in audit procedures they have been considered and verified from an high-level point of view, for example through the analysis of the related policy or procedures.
- Distribution of audit methods: in general, as could be expected, the interview was the method used in every procedure while the analysis of the configuration is almost totally absent, except for two controls cases in which it was applicable and successfully used.

5.2 People controls

5.2.1 Introduction

People controls are presented in Clause 6 of ISO/IEC 27002 document, collecting 8 controls which concern general control aspects related to the security depending on personnel involved in activities that have a relevance in terms of information security, so the correct implementation of such controls contributes to the overall information system security. Through a simple overview of the attributes, it is clear that people controls are mostly preventive and they operate on governance and ecosystem security domains, with the same purpose of protecting information.

The implementation of these controls allows an effective isolation of all those aspects strictly related to individuals, which is why this type of controls mainly groups all those characteristics that depend on the relationship with the people they have to handle information together with the related responsibilities in terms of security. As suggested by the *Operational capabilities* attribute, the purpose of people controls is devoted to provide an adequate level of protection for the human resources: in the corresponding procedures the auditor's objective is ensuring that the necessary means and measures are in place in order to guarantee a safe management of personnel by the organization.

The next subsections will present the developed audit procedures.

5.2.2 Audit procedures

6.1 Screening

- Control: *"Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks."* [11]

The auditing of this control implementation requires the analysis of procedures and activities that are typically carried out by the human resource department. The developed audit procedures aim to interview and analyse documents about the screening process and about the evaluation of competence suitability related to specific information security roles. In addition, the execution of periodic verification checks has been analysed with a dedicated audit procedure.

6.2 Terms and conditions of employment

- Control: *"The employment contractual agreements should state the personnel's and the organization's responsibilities for information security."* [11]

This control aims to ensure that the personnel has been made aware of the importance of their assigned roles and related responsibilities, especially in terms of information security. For this purpose, the developed audit procedures analyse employment contracts management and content in order to assess the clarity of contractual obligation for different roles and the inclusion of fundamental information security related clauses.

6.3 Information security awareness, education and training

- Control: *"Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function."* [11]

Information security awareness is a difficult specification to be evaluated in a quantitative manner, thus the strategy adopted should resort to the evaluation of the means

used to provide awareness. For this purpose, information security awareness programme is subject to audit to verify that it is in line with the organization's policies, while the topics that have to be covered are evaluated in a separate audit procedure. The effectiveness of awareness training can be verified reviewing records of information security awareness sessions evaluations of understanding. In addition, audit procedures have been developed to assess education and training programme update and the information security skills of the technical staff, respectively. The full detailed version of the procedures can be found in Annex B.

6.4 Disciplinary process

- Control: *"A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation."* [11]

In order to ensure that the personnel is made aware of consequences of information security policy violation, a disciplinary process is formalized and verified during the audit through the analysis of related documentation and the observation of disciplinary process records based on the collected violation evidence. In addition, audit procedures have been developed for evaluating the graduated response to the breach and the consideration of relevant legislation, regulations, contractual and business requirements, respectively. In this control documentation and observation methods have been adopted for all developed audit procedures.

6.5 Responsibilities after termination or change of employment

- Control: *"Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties."* [11]

The auditing of this control aims to verify that the validity of responsibilities and duties after termination or change of employment is imposed through the inclusion of corresponding clauses in employment contracts. In addition, audit procedures have been developed for assessing the transfer of roles and responsibilities from an individual leaving or changing job and for verifying how interested parties are notified about that.

6.6 Confidentiality or non-disclosure agreements

- Control: *"Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties."* [11]

This control deals with the management of confidentiality or non-disclosure agreements: the auditors have to analyse the contracts to verify the proper inclusion of confidentiality or non-disclosure clauses and the related content, thus two separate audit procedures have been defined both performed through documentation templates analysis

and review of the agreements. Furthermore, the execution of periodic reviews of the agreements has been verified in a dedicated audit procedure through interview and observation of records relating to recent reviews.

6.7 Remote working

- Control: *"Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises."* [11]

In this context, a topic-specific policy is defined and properly verified in its content suitability and coverage of important security aspects, through the analysis of the documentation that regulates remote working. In addition, an audit procedure has been developed to verify the equipment and related security guidelines for remote working activities and, in this case, the configuration method has been applied for the analysis of configured remote equipment. The full detailed version of the procedures can be found in Annex B.

6.8 Information security event reporting

- Control: *"The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner."* [11]

The implementation of information security event reporting is complementary to the corresponding organizational control described by clause 5.24. In the context of this control, the target of the assessment is the event reporting procedure awareness: the auditor purpose is verifying that users and personnel report information security events as quickly as possible and they are aware of the interested point of contact.

5.2.3 Considerations

The presented people controls cover basic themes and aspects directly involving the personnel: their implementation is mainly devoted to analyse agreements or verify the awareness of such individuals and associated responsibilities that have a relevance in terms of information security. In the developed audit procedures, the objective is ensuring that the necessary means are in place in order to guarantee a safe management of personnel by the organization. For this reason, the procedures individually use as many methods as possible in order to collect evidence of different types. An example of this is the fact that very often when contracts are examined, first an inspection of the template is performed and then a sample of actual corresponding contracts is reviewed. A general overview of developed audit procedures highlights a common recurring patterns as regards:

- Specific aspects: in audit procedures where agreements or contracts have been submitted to inspection, the adopted approach has been devised in order to first analyse the corresponding templates and then a sample of agreements or contracts. The

guidance of ISO/IEC 27002 reference document is well-detailed and many times is specified that some aspects could be not applicable, especially in small size organization. In those cases, the strategy adopted in writing the audit procedures has tried to include all the aspects suggested by the guidance, specifying that they are intended to be taken into consideration only if applicable.

- Distribution of audit methods: in general, the utilization of interview, documentation and observation methods is equally distributed and widely adopted among all audit procedures, while the analysis of the configuration is almost totally absent, except for one control case in which it was applicable and successfully introduced.

5.3 Physical controls

5.3.1 Introduction

Physical controls are presented in Clause 7 of ISO/IEC 27002 document, collecting overall 14 controls which concern implementation aspects related to physical protection, which are essential for ensuring information security to the organization. Through a simple overview of the *Operational capabilities* attribute, it is clear that the purpose is almost totally devoted to provide physical security and asset management, an this is perfectly in line with the idea of physical protection measures that contribute to establish a secure system in its entirety.

The implementation of physical controls is important in order to prevent any physical damage which could lead to compromises of the organization's information security. This requires that areas where information are processed in some way accessible should be adequately provided of secure protection measures that prevent any form of threat derived from the external environment. At the same time, the internal environment should also be suitably controlled, thus in this context the controls deal with the whole monitoring and surveillance system that is necessary in order to properly supervise buildings and facilities, especially the most critical areas. The next subsections will present the developed audit procedures.

5.3.2 Audit procedures

7.1 Physical security perimeters

- Control: *"Security perimeters should be defined and used to protect areas that contain information and other associated assets."* [11]

This control aims to ensure a clear definition of physical security perimeters in order to prevent unauthorized physical accesses. For this purpose, the developed audit procedures must be focused on physical security perimeter definition and its robustness. They both have resorted to interview, analysis of asset inventory records together with in-scope buildings planimetries, and confirmatory physical observation. In addition, public access areas have been separately evaluated to verify that unauthorized access to the bordering premises is forbidden.

7.2 Physical entry

- Control: *"Secure areas should be protected by appropriate entry controls and access points."* [11]

The scope of this control includes many aspects and related protection that must be appropriately verified in the audit procedures. The following list of the developed procedures topics have always resorted to interview and physical observation:

- Maintenance of Physical logbook of all accesses and completeness of the related records
- Activities and duties of the Reception area personnel and related observation
- Adoption and management of Badges, observation of the authorization correctness of badge readers and analysis of the corresponding badge configuration system
- Physical key management and observation of the related physical key logbook
- Deployment of Additional authentication factors and observation of the related utilization and behaviour
- Personnel identification, distinguishing between onsite and visitors
- Visitors authorization procedures and related management during the whole visit
- Delivery and loading areas identification and corresponding separation with respect to other parts of the buildings
- Incoming goods inspection and related observation of tracking records

The full detailed version of the procedures can be found in Annex C.

7.3 Securing offices, rooms and facilities

- Control: *"Physical security for offices, rooms and facilities should be designed and implemented."* [11]

The design of protection measures applied to offices, rooms and facilities contributes to the prevention carried out by physical security perimeters definition of the clause 7.1. In this context, the audit verification especially regards critical facilities' public accessibility and indications of buildings: the developed audit procedures focus on assessing, respectively, the visibility of reserved activities from the outside of critical facilities and the avoided presence of indications of processing activities, when not necessary.

7.4 Physical security monitoring

- Control: *"Premises should be continuously monitored for unauthorized physical access."* [11]

This control implementation includes several protection means that must be appropriately verified. The developed audit procedures aim to inspect the surveillance system and related access rights through the analysis the related monitoring reports and in-scope buildings planimetries. In particular, dedicated procedures have been developed for the verification of CCTV [3] and contact, sound or motion detectors, while the alarm system installation and securing must be properly assessed and reviewed. Furthermore, the collection of personal data for monitoring purposes must comply with laws and regulations, thus the recording policies have been properly evaluated by the auditor.

7.5 Protecting against physical and environmental threats

- Control: *"Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented."* [11]

The implementation of protection measures against physical and environmental threats is directly derived from risk assessment activities, and this correlation is properly verified during the auditing of this control. In this context, the related management should be supported by specialist advices and the physical premises location should be taken into account when identifying the threats. In addition, specific audit procedures have been developed to assess the suitability of the deployed safeguards against fire, flooding, electrical surges, explosive and weapons. For each testing procedure within this control, the verification approaches have always resorted to interview and observation methods.

7.6 Working in secure areas

- Control: *"Security measures for working in secure areas should be designed and implemented."* [11]

The protection of information and other associated assets should be supported by the arrangement of secure areas within the organization, preventing damage and potential interference by personnel. For this purpose, supervision of working should always be provided, secure areas must be adequately managed and the access to information by the personnel should implement the need-to-know principle. All these aspects have been properly addressed in dedicated audit procedures.

[3] Closed-Circuit Television Camera

7.7 Clear desk and clear screen

- Control: *"Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced."* [11]

In auditing this control implementation, a topic-specific policy on clear desk and clear screen is defined and properly verified in its content suitability through the analysis of documentation. Since the evaluation of user endpoint devices protection has been concerned in audit procedures of clause 8.1, in the context of this control the analysis mainly focuses on printers and vacating facilities management involving critical and sensitive information and the related physical protection.

7.8 Equipment siting and protection

- Control: *"Equipment should be sited securely and protected."* [11]

The adequate siting and protection of equipment contributes to reduce the risks from physical and environmental threats. During the assessment, the auditor should evaluate the suitability of equipment and processing facilities location, the related conditions monitoring and associated controls implemented against threats: for this purpose, distinct audit procedures have been developed for the related evaluation. In addition, separation of facilities has been properly addressed by a dedicated procedure that aims to verify the segregation of facilities under the organization control with respect to the ones within shared environments.

7.9 Security of assets off-premises

- Control: *"Off-site assets should be protected."* [11]

The information protection must extended in order cover in-site and off-site assets, thus the latter must be properly identified within the scope of assets inventory, including both devices owned by the organization and private ones, when used on behalf of the organization. For this purpose, audit procedures have been developed to assess their correct identification, the adoption of information security measures for permanently off-site equipment, the chain of custody maintenance and the personnel behaviour awareness as regards the use of off-site devices.

7.10 Storage media

- Control: *"Storage media should be managed through its life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements."* [11]

The management of storage media is a fundamental requirement for information security, thus a topic-specific policy on storage media management is defined and properly verified in its content suitability through the analysis of documentation. In addition, the

following aspects related to storage media have been assessed in distinct audit procedures, which have always resorted to interview and physical observation:

- Removable storage media identification and inclusion during assets classification and inventory
- Availability of safe storage environment for removable storage media
- Application of cryptographic protection depending on the classification of stored information
- Degradation handling and observation of applied prevention measures
- Managements of secure reuse and disposal

The full detailed version of the procedures can be found in Annex C.

7.11 Supporting utilities

- Control: *"Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities."* [11]

The adoption of supporting utilities is a measure that must be properly assessed during audit activities through the evaluation of the deployed equipment: it is adequately separated from the information processing facilities, it should respect relevant manufactorer's specifications and it should be regularly inspected. In addition, utilities appraisal and control and emergency management have been properly analysed through dedicated audit procedures.

7.12 Cabling security

- Control: *"Cables carrying power, data or supporting information services should be protected from interception, interference or damage."* [11]

The physical protection of cables is a basic requirement that aim to prevent any interception, interference or damage. For this purpose, the auditor should verify through interview and observation that the organization has properly addressed cable labelling, interference prevention and power and telecommunications lines protection. In particular, a separate audit procedure has been developed to analyse additional protection measures dedicated to critical or sensitive systems.

7.13 Equipment maintenance

- Control: *"Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information."* [11]

The adequate maintenance of equipment is essential to guarantee stable and long-lasting protection over time. In order to successfully achieve this objective, authorized personnel should carry out the maintenance on equipment according to supplier's maintenance recommendations. Consequently, the adoption of authorized personnel and supplier recommendations have been separately verified in dedicated audit procedures through interview and review of a sample of equipment maintenance records.

7.14 Secure disposal or re-use of equipment

- Control: *"Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use."* [11]

This control aims to prevent any leakage of information deriving from equipment to be disposed or re-used. For this purpose, the two developed audit procedure focus on the equipment analysis to be performed, on one side, before disposal or re-use and, on the other side, on damaged equipment in order to decide whether to destroy or repair it. Specifically, both procedures resort to interview to responsible personnel and review of a sample of performed equipment analysis.

5.3.3 Considerations

The presented physical controls cover basic themes and aspects directly involving the equipment, facilities and buildings of the audited organization: their implementation is devoted to achieve information security, but not only that, through physical protection measures. As previously introduced, the purpose of these controls and the corresponding audit procedures, is to prevent any type of physical damage and threats. For this purpose, it has been considered appropriate to adopt the observation as the predominant testing method and consequently the physical inspection has been largely deployed. This trend reflects the intrinsic property of physical protections which, if present, should be verified in their relevance and effectiveness, thus the audit procedures have been developed with this perspective. A general overview of them highlights common recurring patterns as regards:

- Topic-specific policies: they have always been analysed through interview and documentation analysis, so the corresponding audit procedure has resorted to verbal and documented evidence, by verifying that the policy is established and communicated to all relevant interested parties.

- Specific aspects: in this context, several audit procedures have been developed within the scope of a single control in order to verify specific protection measures separately. In this way, it has been paid the attention to a greater number of details instead of grouping them all in a single audit procedure.

- Distribution of audit methods: the utilization of interview and observation methods is equally distributed and almost always adopted among all audit procedures, while

the analysis of the configuration is almost totally absent, except for two control case in which it was applicable and successfully used. In particular, in the context of physical controls, the observation method consist in physical inspection which permits the auditor to collect physical evidence, which guarantees the highest level of reliability.

5.4 Technological controls

5.4.1 Introduction

Technological controls are presented in Clause 8 of ISO/IEC 27002 document, collecting overall 34 controls which concern practical implementation aspects related to information security. Through a simple overview of the *Security domains* attribute, it is clear that the purpose is almost totally devoted to provide protection, an this is perfectly in line with the idea of technical operational measures of information security. As the other classes of controls, a proper implementation of technological controls ensures a significant reduction of risks in terms of Confidentiality, Integrity and Availability properties.

Since these controls cover many functionalities related to technical aspects, it is not easy to further group them: they overall concerns access control, authentication, network and data protection, backup mechanisms, logging and monitoring. Specifically, some technological controls have a complementary nature with respect to the organizational ones: typically, in the former the scope of the verification is exclusively for technical implementation choices, while the latter are focused on the management of such aspects by the organization. The coverage of information security related themes is very wide and inclusive, just as the guidance of ISO/IEC 27002 is well-detailed and it has been taken as a fundamental reference for the development of the audit procedures. The next subsections will present them.

5.4.2 Audit procedures

8.1 User endpoint devices

- Control: *"Information stored on, processed by or accessible via user endpoint devices should be protected."* [11]

This control deals with the necessary information protection in terms of storage, processing and access, against the risks deriving from the use of user endpoint devices. For this purpose, testing procedures have been grouped in four macro categories, as suggested by the related guidance:

- General: for secure endpoint management, a topic-specific policy is defined and properly verified in its content suitability, through the analysis of the documentation, while the second audit procedure verifies that the list of user endpoint devices is properly maintained and inclusive.

- User responsibility: these audit procedures aim to evaluate aspects derived from user responsibility in using endpoint devices safely, especially in terms of policy awareness and best practices for devices usage in public areas, session termination and endpoint devices lock. The latter two should be enforced by configuration settings that impose session termination timeouts and automatic device locking.
- Personal devices: the separation of personal and business use in personal devices is verified through the configured isolation measures, while licenses agreements are examined in order to assess software licensing.
- Wireless connections: interview, analysis of procedures for configuring wireless connections and a sample of actual configurations are the approaches adopted by the developed audit procedure.

8.2 Privileged access rights & 8.3 Information access restriction

- Control: *"The allocation and use of privileged access rights should be restricted and managed."* [11]
- Control: *"Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control."* [11]

The authorization process for the allocation of privileged access rights (8.2) and for the access to information (8.3) must reflect the topic-specific policy on access control. This implies that privileged user ID assignment rights are evaluated by the auditor considering individual's job function and related responsibilities since assigning privileged rights requires higher authentication requirements and user awareness. Privileged rights should have an expiration and should be periodically reviewed: the developed audit procedures verify these aspects examining a sample of privileged users. As far as administrative rights are concerned, their utilization should be restricted, especially for generic administrator user IDs, so the audit procedure is devoted to verify the related rules and configuration, which is set to track the usage of admin rights.

Following these practices, the audit procedures for information access restriction have been developed performing review of configurations about anonymous access, access control system and dynamic access management in order to support related requirements.

8.4 Access to source code

- Control: *"Read and write access to source code, development tools and software libraries should be appropriately managed."* [11]

This control regulates source code access rights management to prevent any form of unwanted change that could alter the expected behaviour. For this purpose, access control mechanisms are applied both for source code and libraries and source code should be managed in terms of versioning and privileges: the developed audit procedures aim to verify the adoption of versioning tools and the inner consistency between versions, and read/write rights granted to personnel needing them only. In this context, logging all

accesses and changes to source code and integrity checks of the source code are effective detection measures that the auditor is required to evaluate.

8.5 Secure authentication

- Control: *"Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control."* [11]

The application of information access restrictions and the topic-specific policy on access control should contribute to secure authentication. The strength of authentication mechanisms and procedures is usually directly proportional to the classification of the information to be accessed, which implies one or more authentication factors. In this control techniques regarding user account, authentication factors and log-on procedure have been considered as macro groups for the definition of audit procedures:

- User account: mainly inspection of configuration settings has been adopted in verifying several aspects of user accounts, such as inactivity timeout, disabling of inactive accounts, lockout policy and third-party account management. Most of the time the related policies have been also analysed or the responsible personnel has been interviewed.
- Authentication factors: since they are required to be combined whenever critical information systems are accessed, the audit procedure evaluates that the number of adopted authentication factors is adequate to the criticality of such systems, and this is verified through interview, configuration settings analysis and observing a sample of performed critical authentications.
- log-on procedure: log-on procedure requires to be secure enough to prevent unauthorized access and many aspects that could lead to authentication information disclosure are listed in the guidance of ISO/IEC 27002. In particular, the developed audit procedures focus on log-on information disclosure, error messages and previous log-on attempts information which have been assessed through analysis of the system configuration settings and observing a related sample.

The full detailed version of the procedures can be found in Annex D.

8.6 Capacity management

- Control: *"The use of resources should be monitored and adjusted in line with current and expected capacity requirements."* [11]

The management of resources is an aspect that should reflect capacity requirements, which are derived from both functional and business requirements, thus proper identification is one of the objective of the auditing. Since the estimated capacity can be improved to guarantee the efficiency of the systems, it can be dynamically evaluated and periodically submitted through stress-tests or management plans, especially in case of critical systems. In order to verify these aspects, audit procedures have been developed accordingly.

8.7 Protection against malware

- Control: *"Protection against malware should be implemented and supported by appropriate user awareness."* [11]

The implementation of this control ensures protection of information and other associated assets. Since the adoption of malware detection and repair software alone is not enough, an adequate definition of roles and responsibilities, whitelisting and/or blacklisting and several audit procedures regarding anti-malware protection measures are required and subjected to audit verification. Anti-malware tools should be correctly deployed and updated, thus the related assessment is performed through review of anti-malware configuration and observation in a sample of updated protected systems. Similarly, scanning and logging performed by anti-malware tools have been also audited following the same methodology, while anti-malware disabling and messaging coverage have resorted to configuration analysis together with the always present interview with responsible personnel. The full detailed version of the procedures can be found in Annex D.

8.8 Management of technical vulnerabilities

- Control: *"Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken."* [11]

The adequate implementation of this control is part of the wider activities of risk and vulnerability assessment, which are further treated in other ISO standards and are out of the audit scope. Consequently, the developed audit procedures have been devoted to verify the steps of such activities, which have been identified in:

- vulnerability identification: in this context the audit aims to verify the sources of vulnerabilities, which leads to the analysis of asset inventory list and supplied systems contracts. Consequently also technical vulnerability management roles and responsibilities should be assessed.
- vulnerability disclosure: for this purpose, a policy on vulnerability disclosure is defined and the related audit procedure provides for its analysis, including the verification that reporting forms, threat intelligence, information sharing forums are properly used in its process.
- vulnerability evaluation: the audit procedures aim to verify how a vulnerability report is analysed and the adopted response procedures are applied according to change management and information security incident response plans.
- patching: in order to effectively fix or partially solve vulnerabilities through workarounds, a patch should be submitted to audit procedures that verify through interview and observation methods that the organization handles patch authenticity, testing and deployment adequately.

The full detailed version of the procedures can be found in Annex D.

8.9 Configuration management

- Control: *"Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed."* [11]

Configuration management includes several application fields, thus analysing configuration templates is a reasonable choice. In the related audit procedure testing methods have all been applicable to verify their content, their application and their alignment with the asset inventory. In addiction, related periodic reviews should be assessed. In order to assess the whole configuration management process, the audit activities verify how current configurations, logs of the changes and monitoring are handled through interviews and analysis of a sample of configuration records.

8.10 Information deletion

- Control: *"Information stored in information systems, devices or in any other storage media should be deleted when no longer required."* [11]

The deletion of information prevents its exposure when they are no longer needed but this requires it to be performed safely, otherwise it could lead to unexpected disclosures. This is the reason why audit procedures for the verification of secure deletion methods, deletion after retention and deletion of returning equipment have been developed analysing deletion records. Consequently, they contribute in the collection of evidence of successful deletion, which should be properly assessed. In this context, also third-party agreements must be involved in audits of information deletion which must be consistent with organization defined methods.

8.11 Data masking

- Control: *"Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific, and business requirements, taking applicable legislation into consideration."* [11]

The purpose of this control is to guarantee the confidentiality of information through the application of specific techniques. Consequently, the audit procedures have been developed in order to verify the effectiveness of data masking, pseudonymization and anonymization techniques through the observation of their not-reversibility. In particular, since protected data are masked differently depending on users need-to-know, the auditor should verify the coherency of this correlation. The full detailed version of the procedures can be found in Annex D.

8.12 Data leakage prevention

- Control: *"Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information."* [11]

This control handles the risk of data leakage, which should be limited as possible. The developed audit procedures focus on verifying how and what data subject to potential leakage has been classified, monitoring exposing data channels, and analysing data leakage prevention actions such as configuration of deployed prevention tool.

8.13 Information backup

- Control: *"Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup."* [11]

The utilization of backup copies is a fundamental requirement for the availability and the recovery from loss or failure. For this purpose, a topic-specific policy on backup is defined and properly verified in its contents suitability through the analysis of documentation and the related backup plans, while restoration procedures are also subject to observation along with related records. In addition, backup location and storage, its execution and the retention period should be assessed in separate audit procedures which are performed through interview, backup configuration and observation analysis.

8.14 Redundancy of information processing facilities

- Control: *"Information processing facilities should be implemented with redundancy sufficient to meet availability requirements."* [11]

As for backup copies, redundancy is one of the pillar principles that guarantees the availability of information. In the context of this control, it is specifically required for information processing facilities because the purpose is ensuring continuity capability, thus audit procedures have been developed to assess the adequacy of redundancy requirements and the protection of redundant components. In addiction, facilities redundancy, with particular attention to systems and networks, should be verified by analysing the corresponding configurations. A separate procedure has been dedicated to critical services for which system settings should be reviewed, together with the contracts with suppliers.

8.15 Logging

- Control: *"Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed."* [11]

Logging activities are an important detection mechanism that should always support every type of system and associated activities. For this purpose, a topic-specific policy on logging is defined and properly verified in its content suitability through the analysis of documentation. In particular, the set of information and events to be logged consistently with applicable requirements have been respectively assessed in separate audit procedures that review the the policy contents, a sample of system configuration and related produced log information and events. Logs should be safely maintained, which implies that unauthorized log change, integrity protection and retention time are verified in dedicated audit

procedures. Furthermore, log analysis is performed following procedures and supported by threat intelligence, log behavioural patterns and monitoring activities, thus it should be adequately evaluated by the auditor. The full detailed version of the procedures can be found in Annex D.

8.16 Monitoring activities

- Control: *"Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents."* [11]

Monitoring activities are deployed to detect anomalous behaviors which can signal information security incidents. An adequate definition of the baseline behavior is a fundamental requirement that must be appropriately audited through the analysis of the monitoring tools configuration and related sample of records produced by detected anomalous behavior. In a similar way, the elements to be monitored are defined as well, thus their actual monitoring and related configuration settings are subject to audit. In addition, in order to verify third-party account monitoring and alerts generation, audit procedures based on configuration and observation methods have been developed.

8.17 Clock synchronization

- Control: *"The clocks of information processing systems used by the organization should be synchronized to approved time sources."* [11]

This control guarantees the correct interpretation of events and corresponding recorded data which are typically supported by timestamps. For this purpose, in the first audit procedure time sources used for reference clock have been identified, while in the second one clocks of information systems are verified to be correctly synchronized with the reference one through the observation of system timestamps.

8.18 Use of privileged utility programs

- Control: *"The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled."* [11]

In the context of auditing the utilization of privileged utility programs, two audit procedures have been developed which respectively verify the privileged utility programs actual use by authorized personnel only and the limitation their use if not deemed necessary, respectively. The verification is performed through their configuration settings analysis and related observation.

8.19 Installation of software on operational systems

- Control: *"Procedures and measures should be implemented to securely manage software installation on operational systems."* [11]

The secure installation of software is a fundamental requirement for preventing the exploitation of technical vulnerabilities. For this purpose, the developed audit procedures aim to verify that the installation of software is restricted to authorized users only and that supplied software is still supported. In addition, the configuration control system must be reviewed to evaluate that it is configured in order to properly keep track all operational software modifications.

8.20 Networks security

- Control: *"Networks and network devices should be secured, managed and controlled to protect information in systems and applications."* [11]

A secure management of networks and network devices aims to protect information and related processing facilities, thus the analysis of documented network diagram and corresponding configuration files is an important mean for understanding the topology and its correctness. In order to protect the internal organization network from the public one, audit procedures have been developed to verify the application of authentication systems and network filtering, as well as hardening of network devices. In this context it has been deemed appropriate that the auditor takes into consideration the adoption of a segregated network for administration purposes. The full detailed version of the procedures can be found in Annex D.

8.21 Security of network services

- Control: *"Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored."* [11]

This control implementation aims to ensure a secure utilization of network services: the first developed audit procedure focuses on identifying networks and services allowed and authentication requirements under which verifying the application of corresponding firewall rules. The second audit procedure evaluates that the implementation of strong encryption in network devices together with other access control methods is appropriate.

8.22 Segregation of networks

- Control: *"Groups of information services, users and information systems should be segregated in the organization's networks."* [11]

The segregation of networks is a fundamental protection mechanism, as previously applied in clause 8.20 for administration network. In this wider context, the auditor should assess the established criteria of network separation and verify their effective application, by reviewing the division in sub-domain described in network schemes and the related devices configuration. Since wireless networks do not have well-defined network perimeter, they require separate analysis in order to verify the effective segregation from other networks.

8.23 Web filtering

- Control: *"Access to external websites should be managed to reduce exposure to malicious content."* [11]

This control aims to reduce the risk of compromise by malware spread through external websites. For this purpose, connections to malicious websites should be blocked and the related audit procedure should verify that all malicious sources are considered and filtered appropriately. In addition, the use of online resources should be regulated, thus a corresponding audit procedure has been developed.

8.24 Use of cryptography

- Control: *"Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented."* [11]

A topic-specific policy on cryptography is defined and properly verified in its compliance with regulations and in its suitability, through the analysis of the documentation and of a sample of cryptography-using systems configurations. Furthermore, the developed audit procedures also aim to evaluate key management, especially analysing the application of related documented procedures and verifying they are appropriately logged. As regards cryptographic keys, the definition of cryptoperiods for all keys and the detection and management of compromised key are to be assessed during the audit of this control. The full detailed version of the procedures can be found in Annex D.

8.25 Secure development life cycle

- Control: *"Rules for the secure development of software and systems should be established and applied."* [11]

The assessment of this control consists in a unique audit procedure that verifies the coverage of several aspects of a secure development life cycle: this is performed through the assessment of formalized rules established for secure software development and observing the actual implementation within the developers' environment.

8.26 Application security requirements

- Control: *"Information security requirements should be identified, specified and approved when developing or acquiring applications."* [11]

The application security requirements typically derive from risk assessment activity and thus they cover wide range of aspects. The subdivision suggested by the ISO/IEC 27002 guidance has been followed generating three audit procedures based on the observation method: in the first audit procedure the general topics coverage of the application security requirements has been identified through a checklist. The second one specifies a list of requirements for transactional services and the third procedure adopts the same approach to electronic ordering and payment.

8.27 Secure system architecture and engineering principles

- Control: *"Principles for engineering secure systems to be established, documented, maintained and applied to any information system development activities."* [11]

This control purpose aims to ensure the integration of an security-oriented approach within the development life cycle, thus it can be considered as a complementary part of clause 8.25. In this context it is important to verify the definition and related application of security engineering principles, through proper analysis of the documentation and observation of information security engineering activities. In addition, for a secure system architecture, an audit procedure has been developed to evaluate that the secure engineering principles properly consider architectural, infrastructural and technological requirements.

8.28 Secure coding

- Control: *"Secure coding principles should be applied to software development."* [11]

The application of secure coding principles is a basic requirement, needed for reducing the introduction of software vulnerabilities. In the developed audit procedures interview and observation methods have always been adopted. First of all, the auditor should verify that an adequate governance is provided for secure coding by interviewing the responsible personnel and observing a sample of actual development projects. Secure coding should be addressed in three different moments, which are before, during and after coding:

- before: it includes audit procedures regarding appropriate developers' training on secure coding and secure design and architecture.
- during: the audit procedure on secure coding guidelines verifies the suitability of practises and techniques and their consistent adoption.
- after: the audit procedure on code maintenance verifies several aspects of projects maintenance phase, such as updates,logging, vulnerability scanning and libraries management.

The full detailed version of the procedures can be found in Annex D.

8.29 Security testing in development and acceptance

- Control: *"Security testing processes should be defined and implemented in the development life cycle."* [11]

Testing is a fundamental phase of the development process, and specifically in the context of this control, security testing is considered. In the developed audit procedures interview and observation methods have always been adopted. From the auditor point of view, it is important to evaluate the test coverage of security functions, coding and configurations, and the test types which should include source code analysis, vulnerability assessment and penetration testing. This verification is performed reviewing a sample

of results of software security testing. Consequently, tests should be planned including relevant activities and the effort should be prioritized according to the importance of the system under evaluation. As regards the tests execution, they should be performed through adequate tools by personnel independent from the developers team and within multiple execution environments in order to guarantee separation of duties and reflect the deployment environment, respectively.

8.30 Outsourced development

- Control: *"The organization should direct, monitor and review the activities related to outsourced system development."* [11]

This controls deals with addressing information security measures in an outsourced development scenario. For this purpose, a unique audit procedure is in charge of identifying the outsourced activities and analysing the related definition of requirements and expectations which have been agreed by the organization and the external provider. The auditor should review the agreements to verify that they cover fundamental security aspects and how outsourced systems are monitored.

8.31 Separation of development, test and production environments

- Control: *"Development, testing and production environments should be separated and secured."* [11]

The separation of development, test and production environments is an important requirement for preventing production environment from being compromised by uncontrolled activities. Two audit procedures assess the separation of development and production environment and verify the realization of their inner respective security controls, obtaining related evidence. In addition, the auditor should evaluate authorization procedures for the deployment of software, verifying its preventive testing in a separate environment.

8.32 Change management

- Control: *"Changes to information processing facilities and information systems should be subject to change management procedures."* [11]

This control includes a plenty of previous controls' activities that are subject to changes and that must be considered in this implementation scope. From the auditor point of view, a unique audit procedure covers the verification of ICT and software change control procedures that must include for example the impact of changes, their acceptance tests and their deployment plans. The full detailed version of the procedures can be found in Annex D.

8.33 Test information

- Control: *"Test information should be appropriately selected, protected and managed."* [11]

In the context of testing, the selection of relevant information submitted to test activities is fundamental: for this purpose, audit procedures have been developed for assessing test information selection criteria through interview and observation, and for verifying the related applied protection by reviewing the configuration of the environment where test information is used.

8.34 Protection of information systems during audit testing

- Control: *"Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management."* [11]

This control regards the audit activity itself, in whatever form it is performed, which must be agreed by both parties. The developed audit procedures aim to assess how audit requests are managed and how the audit rights are granted while maintaining adequate protection and monitoring through audit trails. Consequently, audit scheduling should be verified also taking into consideration its effects on system availability.

5.4.3 Considerations

The presented technological controls cover many aspects related to technical functionalities. As previously introduced, some technological controls are complementary with respect to the organizational ones, and this trend has been observed also in the guidance of controls. For this reason, where two controls dealt with complementary aspects of the same subject, it has been decided to develop the related procedures exclusively in one or the other control, in order to avoid overlapped verifications and optimize the audit activity.

Since in this context the auditor objective is to focus to all those aspects strictly related to implementation details, the audit procedures related to this type of controls mainly use configuration and observation methods. A general overview of the related developed audit procedures highlights some common recurring patterns as regards:

- Topic-specific policies: they have always been analysed through interview and documentation analysis, so the corresponding audit procedure has resorted to verbal and documented evidence, by verifying that the policy is established and communicated to all relevant interested parties and that it contains and properly regulates the fundamental related requirements. When applicable, the analysis of the configuration has also been performed in order to collect technical evidence, which are more reliable than the ones gathered previously.

- Procedures and processes: in the audit procedures that analyse procedures or processes adopted internally, in addition to the interview, sometimes documentary review and sometimes observation have been used: this choice was dictated purely by pragmatic and realistic considerations since it depends on whether procedures and processes have been formalized or not.
- Specific aspects: depending on the type of analysis to be performed, some aspects have been unified under the same audit procedure, while others have been split in separate procedures. The determining factor has been reasoning on the actual ease of applicability of the procedure by the auditor, taking into consideration practical aspects on time and effort.
- References to additional ISO standards: in several controls, such as the ones relating to access management and key management, further detailed guidance can be found in other ISO standards.
- Distribution of audit methods: in general, as could be expected, the configuration and observation methods have been widely adopted since they adequately examine practical and operational aspects of the actual implementation of control requirements. They are usually used in a joint manner, which implies that typically what is verified analysing configuration settings is then confirmed by the observation of actual results. Consequently, many times interview has been avoided due to the fact that in audit procedures where purely practical aspects have to be assessed, more reliable methods are sufficient to obtain reliable evidence, saving time and resources.

Chapter 6

Conclusion

This final chapter shows the result obtained by the thesis work and introduces a possible future use of the developed procedures towards the standardization of the assessment of information security controls.

6.1 Review and final version

The initial development of the audit procedures has produced an extended early version where a large number of aspects have been considered within each control scope and consequently included in the corresponding procedures. The following step of review has been focused on maintaining a general attitude with respect to the level of detail of involved aspects, reflecting the wide applicability typical of ISO/IEC 27002. This has implied that:

- topics belonging to specific contexts have not been included as testing procedures in order to ensure that they were applicable to organizations of all types and sectors as required by ISO standards;
- the relevance of considered aspects has been a determining factor for their inclusion or exclusion, leading to develop audit procedures just for the main ones;
- detailed control points belonging to separate audit procedures have been aggregated in a unique procedure with a common purpose including more than one aspect to be evaluated.

Specifically, where two controls dealt with complementary aspects of the same subject, it has been decided to develop the related procedures exclusively in one or the other control, in order to avoid overlapped verifications and optimize the audit activity. By way of example, the password management system and the related verification procedures have been handled entirely in auditing of clause 5.17 - Authentication information, although it is also considered in clause 8.5 - Secure authentication.

The utilization of audit methods that provide different levels of assurance can be considered a beneficial strategy: overall, the interview has been the most widely adopted

method because almost in every context it was applicable, and it is flexible and fast, while in order to support the verbal evidence, at least one of the three other methods have been successfully employed.

As far as critical or extended controls are concerned, testing procedures have usually been maintained more precise, leading to obtain on average more that four or five procedures related to a single control implementation. All these choices have been applied pursuing the objective of improving the applicability of the developed audit procedures, which derives from a practical need of optimizing the audit activity. Consequently, the final version is anyway comprehensive and precise enough to give a substantial support in performing audit of information security controls implementation within a real context.

6.2 Future use as contribution to ISO/IEC 27008

In the developed procedures, the essential implementation aspects have been identified as the objective of the verification process, aiming to support the practical audit activities. The innovative organization of information security controls into four thematic areas highlights the 360 degrees protection provided by the implementation of ISO/IEC 27002 standard and, consequently, the high coverage of their assessment. In principle, the ultimate purpose of the developed procedures is devoted to introduce a high degree of homogeneity in the final results, especially in audit findings and related considerations. What has been produced is a good balance between detailed procedures to be followed by auditors and the guidance of controls implementation, taking always into consideration the general attitude of ISO/IEC 27002.

As already mentioned, the nearest published guidance that is close to satisfy this necessity is represented by ISO/IEC 27008 document, even if the current version actually does not provide a detailed baseline. As a Technical Specification deliverable, it is not a full standard but in the future it could become one if properly organized and improved in its contents. For this purpose, the solution proposed in this thesis work has a structure ready to be sent to ISO as a contribution to ISO/IEC 27008 in order to improve, integrate and enhance the table of practice guide for information security assessment. Furthermore, the recent publication of the new version of ISO/IEC 27002 with its better organization of controls will probably increase the adoption of such document and consequently, when auditing implemented controls, a precise guideline enhanced by the developed procedures and aligned with such structure will be positively affected.

ISO/IEC 27008 has recently started its revision process for transitioning from the old to the new version of ISO/IEC 27002. The developed testing procedures have been handed over to the Italian national body (UNINFO CT 510) that institutionally takes part to this revision via its chairman, Dr. Fabio Guasconi, so that it can be integrated within the italian contribution towards its improvement, and has been warmly received as "a very interesting piece of work which deserves to be used and promoted at an international level".

Appendix A

Organizational procedures

ID	5.8
Testing Procedure	**Information security risks**
Interview	Interview responsible personnel to verify how information security risks are part of the project risks from the early stages and are object of treatment and review.
Document	
Configuration	
Observation	Observe project risks assessment to verify that information security risks have been included from their early stages and adequately treated and reviewed.
Testing Procedure	**Information security requirements definition**
Interview	Interview responsible personnel to verify how information security requirements have been derived for the project.
Document	
Configuration	
Observation	Observe that project information security requirements have been derived by: 1) information security or topic-specific policies 2) threat modelling 3) incidents reviews 4) vulnerability thresholds 5) contingency planning
Testing Procedure	**Information security requirements consideration**
Interview	Interview responsible personnel to verify what information security requirements have been taking into consideration within the project.
Document	
Configuration	
Observation	Observe that project information security requirements have been considering: 1) involved information and required protection 2) level of assurance required for authentication 3) access provisioning and authorization processes 4) user information on duties and responsibilities 5) business processes inputs 6) mandates by other controls 7) legal, statutory, regulatory and contractual environment 8) level of assurance required to third parties

ID	5.11
Testing Procedure	**Asset return formalization**
Interview	Interview responsible personnel to verify how the termination process has been formalized to include the return of all assigned assets
Document	Analyse relevant policies and procedures to verify that the return of all assigned assets upon termination is formalized
Configuration	
Observation	
Testing Procedure	**Information deletion**
Interview	Interview responsible personnel to verify how information deletion is performed on returned assets or personal assets being used by terminated personnel
Document	Analyse relevant procedures to verify how information deletion is required to be performed on returned assets or personal assets being used by terminated personnel
Configuration	
Observation	
Testing Procedure	**Knowledge return**
Interview	Interview responsible personnel to verify how knowledge of terminated personnel is transferred back to the organization
Document	
Configuration	
Observation	Review documented information about returned knowledge from terminated personnel
Testing Procedure	**Prevent unauthorized copies**
Interview	Interview responsible personnel to verify how unauthorized copies are prevented during the notice period and after termination
Document	
Configuration	
Observation	Review measures in place to prevent unauthorized copies during the notice period and after termination
Testing Procedure	**Returned assets**
Interview	Interview responsible personnel to verify how all assets to be returned are identified including: 1) user endpoint devices 2) personal devices (and portable storage devices) 3) special equipment 4) authentication hardware 5) physical copies of information
Document	
Configuration	
Observation	Review asset return records to match asset return lists
ID	**5.12**
Testing Procedure	**Information classification policy**
Interview	Interview responsible personnel to verify that a topic-specific policy on information classification is established and communicated to all relevant interested parties
Document	Analyse the information classification policy to verify that a scheme for the classification of information including confidentiality, integrity and availability requirements and resulting impacts is defined
Configuration	
Observation	
Testing Procedure	**Access control and business requirements alignment**
Interview	Interview responsible personnel to verify how information classification is aligned with access control policies and with business requirements
Document	Analyse the access control policy and verify its alignment with the information classification policy and with business requirements

Configuration	
Observation	
Testing Procedure	**Consistency across organization procedures**
Interview	Interview responsible personnel to verify that the information classification scheme is established and included in organization procedures
Document	Analyse information classification procedures to verify they allow a consistent application of information classification across the organization
Configuration	
Observation	
Testing Procedure	**Interoperability with other organization's schemes**
Interview	Interview responsible personnel to verify that agreements with other organizations include a way to interpret different classification schemes
Document	
Configuration	
Observation	Review agreements with other organizations to verify they include procedures to identify the classification of information and to interpret the classification levels from other organizations
Testing Procedure	**Review of information classification scheme**
Interview	Interview responsible personnel to verify how information classification is required to be reviewed over time accordingly to change in terms of value, sensitivity or criticality
Document	Analyse the information classification policy to verify that information classification is required to be reviewed over time accordingly to change in terms of value, sensitivity or criticality
Configuration	
Observation	
ID	**5.13**
Testing Procedure	**Labelling procedures definition**
Interview	Interview responsible personnel to verify that labelling procedures are in place and are distributed to all personnel
Document	Analyse labelling procedures to verify that they cover information and other associated assets in all formats, coherently with the established information classification scheme.
Configuration	
Observation	
Testing Procedure	**Labels application**
Interview	Interview responsible personnel to verify they know: 1) how to label information, depending on the format 2) how to handle impossible labelling 3) when labelling can be omitted
Document	
Configuration	
Observation	Review a sample of classification labels to verify that they are: 1) coherent with the classification scheme 2) clear and easily recognizable 3) applied to the appropriate information assets in the appropriate place(s)
Testing Procedure	**Metadata**
Interview	Interview responsible personnel to verify that labelling procedures include: 1) how to attach metadata to information 2) what labels to use 3) how data are handled
Document	Analyse labelling procedures to verify that they include descriptions on how to attach metadata to information and what metadata to attach.
Configuration	
Observation	

Testing Procedure	**Metadata application**
Interview	Interview responsible personnel to verify they know how to apply metadata and what metadata to apply to information
Document	
Configuration	
Observation	Review a sample of metadata to verify that they: 1) are coherent with the classification scheme 2) are applied to the appropriate information assets in the appropriate way 3) include metadata used by systems to process information depending on theur information security properties
ID	**5.14**
Testing Procedure	**Information transfer policy definition**
Interview	Interview responsible personnel to verify that a topic-specific policy on information transfer is established and communicated to all interested parties
Document	Analyse the information transfer policy to verify that information transfer is documented and established through rules, procedures and agreements
Configuration	
Observation	
Testing Procedure	**General information transfer agreements**
Interview	
Document	Analyse information transfer documented rules and procedures to verify they include: 1) controls designed to protect transferred information and to ensure traceability and non-repudiation 2) identification of appropriate contacts related to the transfer 3) responsibilities and liabilities in the event of information security incidents 4) use of an agreed labelling system for sensitive or critical information 5) retention and disposal guidelines for all business records
Configuration	
Observation	Review a sample of information transfer agreements to verify they include: 1) controls designed to protect transferred information and to ensure traceability and non-repudiation 2) identification of appropriate contacts related to the transfer 3) responsibilities and liabilities in the event of information security incidents 4) use of an agreed labelling system for sensitive or critical information 5) retention and disposal guidelines for all business records
Testing Procedure	**Electronic information transfer agreements**
Interview	
Document	Analyse electronic information transfer documented rules and procedures to verify they additionally include: 1) detection of and protection against malware that can be transmitted 2) protection of attachments 3) prevention against sending information to wrong recipients 4) obtaining approval prior to using external public services 5) stronger levels of authentication when using publicly accessible networks 6) restrictions associated with electronic communication facilities 7) advising personnel and other interested parties not to send SMS or instant messages with critical information 8) advising personnel and other interested parties about the problems of using fax machines or services
Configuration	

Observation	Review a sample of electronic information transfer agreements to verify they include: 1) detection of and protection against malware that can be transmitted 2) protection of attachments 3) prevention against sending information to wrong recipients 4) obtaining approval prior to using external public services 5) stronger levels of authentication when using publicly accessible networks 6) restrictions associated with electronic communication facilities 7) advising personnel and other interested parties not to send SMS or instant messages with critical information 8) advising personnel and other interested parties about the problems of using fax machines or services
Testing Procedure	**Physical information transfer agreements**
Interview	
Document	Analyse physical information transfer documented rules and procedures to verify they additionally include: 1) responsibilities for controlling and notifying transmission, dispatch and receipt 2) ensuring correct addressing and transportation of the message 3) packaging protecting the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications 4) a list of authorized reliable couriers agreed by management and courier identification standards 5) tamper evident or tamper-resistant controls 6) procedures to verify the identification of couriers 7) approved list of third parties providing transportation 8) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorised recipients, the times of transfer to the transit custodians and receipt at the destination
Configuration	
Observation	Review a sample of physical information transfer agreements to verify they include: 1) responsibilities for controlling and notifying transmission, dispatch and receipt 2) ensuring correct addressing and transportation of the message 3) packaging protecting the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications 4) a list of authorized reliable couriers agreed by management and courier identification standards 5) tamper evident or tamper-resistant controls 6) procedures to verify the identification of couriers 7) approved list of third parties providing transportation 8) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorised recipients, the times of transfer to the transit custodians and receipt at the destination
Testing Procedure	**Verbal transfer awareness**
Interview	Interview sample personnel to verify that they are aware they should: 1) not have confidential verbal conversations in public places or over insecure communication channels 2) not leave messages containing confidential information 3) begin any sensitive conversations with a disclaimer
Document	
Configuration	

Observation	Review verbal transfer security awareness initiatives records to verify they include indications: 1) not have confidential verbal conversations in public places or over insecure communication channels 2) not leave messages containing confidential information 3) to begin any sensitive conversations with a disclaimer
ID	**5.15**
Testing Procedure	**Access control policy definition**
Interview	Interview responsible personnel to verify that a topic-specific policy on access control is established and communicated to all relevant interested parties
Document	Analyse the access control policy to verify that established requirements consider business, risk and information security and include: 1) determining which entities require which type of access to the information and other associated assets 2) security of applications 3) physical access, which needs to be supported by appropriate physical entry controls 4) information dissemination and authorization and information security levels and classification of information 5) restrictions to privileged access 6) segregation of duties 7) relevant legislation, regulations and any contractual obligations regarding limitation of access to data or services 8) segregation of access control functions 9) formal authorization of access requests 10) the management of access rights 11) logging
Configuration	
Observation	
Testing Procedure	**Access control rules**
Interview	
Document	Analyse documented access control rules to verify that they have taken into account: 1) consistency between the access rights and information classification 2) consistency between the access rights and the physical perimeter security needs and requirements 3) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use; 4) considering how elements or factors relevant to dynamic access control can be reflected.
Configuration	Review configured access control rules to verify they are consistent with the access control policy, the access control principles of need to know and need to use and that they are aligned with the documented access control rules.
Observation	
Testing Procedure	**Access control models**
Interview	Interview responsible personnel to identify what access control model (MAC, DAC, RBAC, ABAC) is adopted and for what systems.
Document	
Configuration	Review configured access control rules to verify they are consistent with the access control model they belong to.

Observation	
ID	**5.17**
Testing Procedure	**Identity verification**
Interview	Interview responsible personnel to verify how the identity of the user to be assigned the authentication information is verified
Document	Analyse the procedure used to verify the identity of user to be assigned the authentication information to ensure that they are not provided without its successful conclusion
Configuration	
Observation	
Testing Procedure	**Receipt**
Interview	Interview responsible personnel to verify how users acknowledge the reception of authentication information
Document	
Configuration	
Observation	Observe a sample of user reception of authentication information acknowledge
Testing Procedure	**Change of default password**
Interview	interview responsible personnel to verify that authentication information provided by vendors is changed immediately
Document	
Configuration	
Observation	Observe a sample of installation to verify that right after installation users are enforced to change authentication information
Testing Procedure	**Confidential password input**
Interview	
Document	
Configuration	Examine the system configuration to verify that functionality that hides the passwords when are being entered is enabled
Observation	Observe how confidentiality of passwords inputed by personnel connecting to systems is provided on the screen
Testing Procedure	**Random password**
Interview	Interview password assignment responsible personnel to understand how initial and to-be-reset passwords are generated differently to each other
Document	
Configuration	
Observation	Observe two or more password assignment or reset processes and how those passwords differ
Testing Procedure	**First password change**
Interview	
Document	
Configuration	Review system configurations to enforce that a password change is required when a new account is created or its password is reset
Observation	Observe the presence of a change password request after personnel connects to a newly created or password-reset accounrt
Testing Procedure	**Password length**
Interview	
Document	Analyse password policies to verify that require a minimum password length
Configuration	Review system configurations to enforce a minimum password length consistent with the policy for all users
Observation	
Testing Procedure	**Password complexity**
Interview	

Document	Analyse password policies to verify that passwords are required to include characters belonging to different types (i.e. lower case, upper case, numbers, special character) and common dictionary words
Configuration	Review system configurations to enforce a password complexity consistent with the policy for all users
Observation	
Testing Procedure	**Password change time**
Interview	
Document	Analyse password policies to verify that require a minimum and a maximum time for password change
Configuration	Review system configurations to enforce minimum and a maximum times for password change
Observation	
Testing Procedure	**Password history**
Interview	
Document	Analyse password policies to verify that already used passwords are prohibited to be reused
Configuration	Review system configurations to enforce passwords difference from already used ones
Observation	
Testing Procedure	**Password storage**
Interview	
Document	
Configuration	Review system configuration settings to render all authentication credentials stored in an unreadable, unreversible fashion
Observation	Observe password storage locations to ensure they are unreadable and unreversible
Testing Procedure	**Password transmission**
Interview	
Document	
Configuration	Review system configuration settings to render all authentication credentials unreadable during trasmission
Observation	Observe eavesdropped network traffic to ensure password transmission is unreadable
ID	**5.18**
Testing Procedure	**Owner and management authorization**
Interview	Interview responsible personnel to verify how owner of information and associated assets grants access rights
Document	
Configuration	
Observation	Review a sample of access right grants to verify they have been duly authorized by the owner of information and associated assets
Testing Procedure	**Segregation of duties**
Interview	Interview responsible personnel to verify how segregation of duties between approver and implementers of access rights is addressed
Document	Analyse function and organizational charts to verify segregation of roles of approval and implementation of access rights
Configuration	
Observation	
Testing Procedure	**Removing rights**
Interview	Interview responsible personnel to verify how access rights that need to be removed are effectively removed
Document	
Configuration	
Observation	Review records of removal of access rights and verify they have been performed correctly and timely

Testing Procedure	**Modifying rights**
Interview	Interview responsible personnel to verify how access rights that need to be modified for job/role change are managed
Document	
Configuration	
Observation	Review records of access rights modification after job/role change and verify they have been performed correctly and timely
Testing Procedure	**Temporary rights**
Interview	Interview responsible personnel to verify how temporary access rights are managed
Document	
Configuration	
Observation	Review records of temporary access rights attribution to verify their correctness and effective expiration
Testing Procedure	**Regular reviews**
Interview	Interview responsible personnel to verify how regular review are performed and with what frequency
Document	
Configuration	
Observation	Review the most recent access rights review report to verify it is regularly performed and it includes: -users' access rights changes -authorization for privileged access rights
ID	**5.20**
Testing Procedure	**Register of supplier agreements**
Interview	Interview responsible personnel to verify that agreements with suppliers are periodically reviewed and maintained in a register
Document	
Configuration	
Observation	Review the register to verify it is kept, the agreements are up-to-date and are cover all relevant products and services supplies
Testing Procedure	**Supplier agreements contents**
Interview	Interview responsible personnel to verify how agreements with suppliers are defined and negotiated

Document	Analyse supplier agreements templates to verify they contain as applicable: 1) classification and description of the information to be provided or accessed and methods of providing or accessing the information 2) legal, statutory, regulatory, contractual, information security (such as incident management, training and awareness, screening, backup, physical security, information transfer), business continuity requirements 3) obligation of each contractual party to implement an agreed set of controls, to periodically deliver a report on the effectiveness of controls, right to audit the supplier processes and controls related to the agreement and agreement on timely correction of relevant issues raised 4) rules of acceptable use of information and other associated assets 5) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel 6) indemnities and remediation for failure of contractor to meet requirements, defect resolution and conflict resolution processes 7) incident management procedures 8) change management process ensuring advance notification to the organization and the possibility for the organization of not accepting changes 9) relevant provisions for sub-contracting, including the controls that need to be implemented 10) relevant contacts, including a contact person for information security issues 11) termination clauses upon conclusion of the agreement and related handover support to another supplier or to the organization itself
Configuration **Observation**	Review supplier agreements to verify they contain as applicable: 1) classification and description of the information to be provided or accessed and methods of providing or accessing the information 2) legal, statutory, regulatory, contractual, information security (such as incident management, training and awareness, screening, backup, physical security, information transfer), business continuity requirements 3) obligation of each contractual party to implement an agreed set of controls, to periodically deliver a report on the effectiveness of controls, right to audit the supplier processes and controls related to the agreement and agreement on timely correction of relevant issues raised 4) rules of acceptable use of information and other associated assets 5) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel 6) indemnities and remediation for failure of contractor to meet requirements, defect resolution and conflict resolution processes 7) incident management procedures 8) change management process ensuring advance notification to the organization and the possibility for the organization of not accepting changes 9) relevant provisions for sub-contracting, including the controls that need to be implemented 10) relevant contacts, including a contact person for information security issues 11) termination clauses upon conclusion of the agreement and related handover support to another supplier or to the organization itself
ID	**5.25**
Testing Procedure	**Categorization and prioritization scheme**

Interview	Interview point of contact personnel to verify what agreed categorization and prioritization scheme is used by the point of contact to classify security events and how it is based on their potential consequences
Document	
Configuration	
Observation	Review a sample of results of the assessment decisions to verify the correct use of the adopted information security categorization scheme
ID	**5.26**
Testing Procedure	**Incident response procedures**
Interview	Interview responsible personnel to verify that incident response procedures are established and are distributed to all relevant interested parties
Document	Analyse incident response procedures to verify they include: 1) affected systems identification 2) collection of evidence 3) requiring crisis management activities and business continuity plans 4) logging of response activities 5) requiring forensic analysis 6) informing interested parties 7) formally closing and recording solved incidents 8) coordination with authorities, external interest groups and forums, suppliers and clients 9) post-incident analysis including root cause 10) vulnerabilities and weaknesses management
Configuration	
Observation	
ID	**5.27**
Testing Procedure	**Procedures to gain incident information**
Interview	Interview responsible personnel to verify that procedures to quantify and monitor types, volumes and costs of information security incidents are established
Document	
Configuration	
Observation	Review a sample of information gathered from security incidents to verify how types, volumes and costs have been quantified and monitored
Testing Procedure	**Incident management improvements**
Interview	interview responsible personnel to verify how incident management has benefited from information gained from the evaluation of security incidents
Document	
Configuration	
Observation	Review performed actions to improve incident management considerations derived from information security incidents experience

Appendix B

People procedures

ID	6.3
Testing Procedure	**Information security awareness programme**
Interview	Interview responsible personnel to understand the structure of the information security awareness programme and to verify that is in line with the organization's policies
Document	Analyse the information security awareness programme to verify that it provides multiple methods and channels, both physical and virtual
Configuration	
Observation	
Testing Procedure	**Information security awareness activities coverage**
Interview	Interview responsible personnel to understand the topics covered by the information security awareness programme and that its outreach comprises all of the organization's staff, with specific regards for the newly hired and relevant third parties
Document	
Configuration	
Observation	Review records of a sample information security awareness initiatives to verify that all the following topics are covered: 1) management's commitment towards information security 2) information security rules and obligations 3) personal accountability for own actions and inactions 4) baseline information security procedures and controls 5) contact points and resources
Testing Procedure	**Information security awareness effectiveness**
Interview	Interview a sample of personnel with different roles to verify they have completed the awareness training retaining the expected knowledge about: -authentication policies, procedures and good practices - how to behave to avoid and contain malware
Document	
Configuration	
Observation	Review records of information security awareness sessions evaluations of understanding to ensure the initiatives are evaluated and effective.
Testing Procedure	**Education and training programme update**
Interview	Interview responsible personnel to understand the education and training programme and to verify that is in line with the organization's policies
Document	Analyse the information security awareness programme to verify that it is aimed to increase specific skill sets and expertise as appropriate for the recipient's job position needs.

Configuration	
Observation	
Testing Procedure	**Technical staff information security skills**
Interview	Interview a sample of technical staff to verify how they keep their technical skills up-to-date
Document	
Configuration	
Observation	Observe records for technical staff participation into conferences and events or subscribing to newsletter and magazines
ID	**6.7**
Testing Procedure	**Remote working policy**
Interview	Interview responsible personnel to verify that a topic-specific policy on remote working is established and communicated to all relevant interested parties
Document	Analyse remote working policy to verify it defines the relevant conditions and restrictions about remote working, including, when applicable: 1) the existing or proposed physical security of the remote working site; 2) rules and security mechanisms for the remote physical environment 3) the expected physical remote working environments; 4) the communications security requirements; 5) the use of remote access such as virtual desktop access that establishes appropriate processing and storage of information on privately owned equipment; 6) the threat of unauthorized access to information or resources from other persons at the remote working site and in public places; 7) the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services; 8) use of security measures, such as firewalls and protection against malware; 9) secure mechanisms for deploying and initializing systems remotely and for authentication and enablement of access privileges
Configuration	
Observation	
Testing Procedure	**Equipment and guidance**
Interview	Interview personnel working remotely to verify which guidelines, communication equipment, storage furniture and devices are provided for remote working activities
Document	Analyse guidance for remote working to verify they include considerations about: 1) physical security 2) family and visitor access to equipment and information 3) backup and business continuity procedures 4) hardware and software support and maintenance 5) accessible information based on classification
Configuration	Review remote equipment configuration to verify it is set to provide: 1) secure remote access methods 2) screen locks and inactivity timers 3) device location tracking 4) remote wipe capability
Observation	

Appendix C

Physical procedures

ID	7.2
Testing Procedure	**Physical logbook**
Interview	Interview responsible personnel to verify that a physical logbook is maintained to document all accesses
Document	
Configuration	
Observation	Review a sample of physical logbook records to verify they are complete with all required information including date and time of entry, accurate and stored for a limited and defined time period only
Testing Procedure	**Reception area**
Interview	Interview the reception personnel to understand their activities and verify their duties
Document	
Configuration	
Observation	Observe the reception area to verify it can continuously control physical access to the site
Testing Procedure	**Badge management**
Interview	Interview the reception personnel to verify what types of badge are adopted to access what secure areas and how they are managed
Document	
Configuration	Review badge configuration system to be configured consistently with access requirements
Observation	Observe how badge readers react to badges not authorized for entry for each secure area
Testing Procedure	**Physical key management**
Interview	Interview responsible personnel to identify what physical keys or combinations are in use and how they are managed
Document	
Configuration	
Observation	Review the physical key logbook to be inclusive of all physical keys or combinations and to fully document their assignments
Testing Procedure	**Additional authentication factors**
Interview	Interview responsible personnel to identify where additional authentication factors such as biometric means or PINs are deployed
Document	
Configuration	
Observation	Observe additional authentication factors use to be in line with its expected behavior and how the access control system reacts to their wrong provision

Testing Procedure	**Personnel identification**
Interview	Interview reception personnel to verify the procedures to distinguish between onsite personnel and visitors
Document	
Configuration	
Observation	Observe a sample of personnel within the site to be distinguishable if onsite personnel or visitor
Testing Procedure	**Visitors authorization**
Interview	Interview reception personnel to verify that visitors are granted access only after being authorized, accompanied and that they surrender any assigned element before leaving the site
Document	
Configuration	
Observation	Observe a sample of visitor records to verify that they have been properly authorized, accompanied and that have surrendered any assigned element before leaving the site
Testing Procedure	**Delivery and loading**
Interview	Interview responsible personnel to identify delivery and loading areas
Document	
Configuration	
Observation	Observe that delivery and loading areas access doesn't allow unauthorized access to other parts of the building
Testing Procedure	**Incoming goods**
Interview	Interview responsible personnel to verify that incoming goods are inspected
Document	
Configuration	
Observation	Review incoming goods registers to verify they are tracked consistently with all other assets
ID	**7.10**
Testing Procedure	**Storage media management policy definition**
Interview	Interview responsible personnel to verify that a topic-specific policy on the management of removable storage media is established and communicated to all interested parties
Document	Analyze the storage media management policy to verify it includes all relevant aspects of the lifecycle of storage media
Configuration	
Observation	
Testing Procedure	**Removable storage media identification**
Interview	Interview responsible personnel to verify how removable storage media are identified during classification and inventory
Document	
Configuration	
Observation	Review asset inventories and verify the removable storage media are adequately identified and included
Testing Procedure	**Safe storage environment**
Interview	Interview responsible personnel to verify how removable storage media are stored in a secure environment that reflects classification of information and manufacturer's specifications
Document	
Configuration	
Observation	Observe a sample of media to be stored accordingly to their classification and to their manufacturer's specifications

Appendix D

Technological procedures

ID	8.5
Testing Procedure	**Authentication policies distribution**
Interview	Interview responsible personnel to verify that authentication policies and procedures are known to all users
Document	
Configuration	
Observation	
Testing Procedure	**Inactivity timeout**
Interview	
Document	Analyse the defined timeout policy parameters and related business needs
Configuration	Inspect system configuration settings on a sample of systems, applications, devices and relevant network sessions to verify that the inactivity period value is consistently configured
Observation	
Testing Procedure	**Inactive account disabling**
Interview	
Document	Analyse the relevant policy to verify the account inactivity period disabling and related business need
Configuration	Inspect system configuration settings to verify that the number of days that define the inactivity period of accounts is set to 90 days or that no accounts with more than 90 days of inactivity are enabled
Observation	
Testing Procedure	**Lockout policy**
Interview	
Document	Analyse the relevant policy to verify that accounts are locked out after a predefined number of wrong attempts for a defined time
Configuration	Inspect configuration settings for a sample of systems to verify that the lockout option is configured consistently with the relevant policy
Observation	
Testing Procedure	**Third-party account management**
Interview	Interview responsible personnel to verify how accounts used for remote access are enabled only when needed and disabled when not in use
Document	
Configuration	Inspect configuration settings for a sample of systems with third-party accounts to verify they are enabled only when needed and disabled when not in use
Observation	

Testing Procedure	**Authentication factors**
Interview	Interview responsible personnel to verify that a number of authentication factor proportional to the system's criticality and profile role is requested for all accesses
Document	
Configuration	Review configuration settings for a sample of systems to verify that the expected number of different authentication factor is required
Observation	Observe personnel connecting to systems being required the expected number of different authentication factor
Testing Procedure	**Log-on information disclosure**
Interview	
Document	
Configuration	Review system configurations to verify that system/application information are not sent and displayed until the user is successfully logged in
Observation	Observe information provided to personnel connecting to systems before and after log-on
Testing Procedure	**Log-on error messages**
Interview	
Document	
Configuration	Review system configurations to verify that when inserted authentication information is wrong, no information about what is wrong is provided
Observation	Observe information provided to personnel connecting to systems after log-ons failing user ID and all used authentication factors
Testing Procedure	**Previous log-on attempts information**
Interview	
Document	
Configuration	Review system configurations to verify that previous valid and invalid log-on attempts are recorded and displayed after successful log-on
Observation	Observe information provided to personnel connecting to systems including previous valid and invalid log-on attempts
ID	**8.7**
Testing Procedure	**White/blacklisting**
Interview	Interview responsible personnel to verify what white/blacklist policy is adopted
Document	
Configuration	Review white/blacklisting configuration settings to be relevant and actual
Observation	
Testing Procedure	**Anti-malware tool deployment**
Interview	Interview responsible personnel to verify what decisions have been made about systems commonly affected by malware
Document	
Configuration	Review anti-malware configuration to verify that it actively protects all commonly affected systems
Observation	Compare the list of systems commonly affected by malware and the ones protected by anti-malware
Testing Procedure	**Anti-malware tool update**
Interview	Interview responsible personnel to verify how the software is kept up to date
Document	
Configuration	Review anti-malware configuration to verify that the software is automatically updated with a suitable frequency
Observation	Observe the last update of anti-malware definitions on a sample of systems
Testing Procedure	**Anti-malware disabling**
Interview	Interview responsible personnel to verify that anti-malware software disabling is not allowed by unprivileged users
Document	

Configuration	Review anti-malware configuration to ensure that its cannot be disabled by unprivileged users
Observation	
Testing Procedure	**Anti-malware scanning**
Interview	Interview personnel to verify that runtime protections are enabled and periodic scans are performed
Document	
Configuration	Review anti-malware configuration to verify that runtime protections are active and periodic scans are planned
Observation	Observe the last periodic scan execution report on a sample of systems
Testing Procedure	**Anti-malware logging**
Interview	Interview personnel to verify that logging is performed and protected from unauthorized access
Document	
Configuration	Review anti-malware configuration to verify that log information on malware related events is recorded and complete
Observation	Observe the presence, the protection and the completeness log entries generated from anti-malware tools
Testing Procedure	**Anti-malware messaging coverage**
Interview	Interview personnel to verify what anti-malware messaging coverage is deployed
Document	
Configuration	Review anti-malware configuration to ensure that scanning of email, attachments and downloads is performed before their use
Observation	
Testing Procedure	**Roles and responsibilities**
Interview	Interview personnel to verify that security policies for protecting systems against malware are in use
Document	Examine security policies for protecting systems against malware to verify that roles and responsibilities are clearly defined
Configuration	
Observation	
ID	**8.8**
Testing Procedure	**Roles and responsibilities**
Interview	Interview responsible personnel to verify that roles and responsibilities for technical vulnerability management are assigned
Document	Verify that roles and responsibilities are formally documented and assigned to competent personnel for each stage of vulnerability management
Configuration	
Observation	
Testing Procedure	**Information resources vulnerabilities**
Interview	Interview responsible personnel to verify how the updated asset inventory list is used as input to identify information resources
Document	
Configuration	
Observation	Cross check asset inventory vendors and models with a sample of identified vulnerabilities to verify the coverage is complete
Testing Procedure	**Vulnerabilities and information systems suppliers**
Interview	
Document	Verify that supplied information systems contracts require to disclose and report vulnerabilities.
Configuration	
Observation	
Testing Procedure	**Vulnerability disclosure policy**

Interview	Interview responsible personnel to verify that vulnerability disclosure policy is defined and distributed to all relevant parties
Document	Analyse vulnerability disclosure policy to verify that it clearly defines procedures that specify to whom, how and when to report vulnerabilities
Configuration	
Observation	Review that reporting forms, threat intelligence, information sharing forums are properly used in the vulnerability disclosure process
Testing Procedure	**Report analysis**
Interview	Interview responsible personnel to verify how reports are analysed to identify which measures are necessary depending on the associated risks
Document	
Configuration	
Observation	Review that report analysis evidence effectively address discovered vulnerabilities
Testing Procedure	**Vulnerability response procedure**
Interview	
Document	Analyse vulnerability response procedure to verify it includes: -priorities for fixing vulnerabilities -tests to confirm mitigation effectiveness -rescans to validate vulnerability absence
Configuration	
Observation	Review vulnerability response actions undertaken to respond to a sample of discovered vulnerabilities
Testing Procedure	**Change management and information security incident response compliance**
Interview	Interview responsible personnel to verify that actions performed to fix vulnerabilities are compliant with change management and information security incident response procedures
Document	Examine a sample for each risk level of the discovered vulnerability to verify that actions respect change management and information security incident response procedures
Configuration	
Observation	
Testing Procedure	**Patch authenticity**
Interview	Interview responsible personnel to verify which are legitimate and trusted sources patches comes from and how are verified to be authentic
Document	
Configuration	
Observation	Observe how patch authenticity verification is performed
Testing Procedure	**Patch testing**
Interview	Interview responsible personnel to verify that testing activities are performed before installing patches in production environments
Document	
Configuration	
Observation	Review patch testing results records to verify their performance
Testing Procedure	**Patch deployment**
Interview	Interview responsible personnel to verify that patch deployment needs to be authorized and is performed on high-risk systems first
Document	
Configuration	
Observation	Review patch deployment authorization presence and installation on high-risk systems first
Testing Procedure	**Workarounds**
Interview	Interview responsible personnel to verify what actions are undertaken when a patch cannot be applied or does not exist yet

Document	
Configuration	
Observation	Review workaround application cases effectiveness
ID	**8.11**
Testing Procedure	**Pseudonymization and anonymization**
Interview	Interview responsible personnel to verify if and how pseudonymization and anonymization techniques are adopted
Document	Identify which elements of a sample of sensitive information are anonymized to verify the effectiveness
Configuration	
Observation	Observe a sample of pseudonymized or anonymized data to verify there is minimal risk of re-identification
Testing Procedure	**Data masking techniques**
Interview	Interview responsible personnel to verify what data masking techniques are applied to what information
Document	
Configuration	
Observation	Observe a sample of masked data to verify masking is performed correctly and it is not reversible
Testing Procedure	**Selective data masking**
Interview	Interview responsible personnel to verify if and how data are masked differently depending on users need-to-know
Document	
Configuration	
Observation	Observe masked data accesses performed by profiles with different need to know to verify the differences are coherent
ID	**8.15**
Testing Procedure	**Logging policy definition**
Interview	Interview responsible personnel to verify that a policy on logging is established and distributed to all interested parties
Document	Analyse the logging policy to verify that the following aspects are identified: -requirements for handling log data -collected and logged data -purpose of logging
Configuration	
Observation	
Testing Procedure	**Information to be logged**
Interview	
Document	Analyse logging policy to verify they require logging a set of information consistent with applicable requirements, including: 1) user IDs; 2) system activities; 3) dates, times and details of relevant events; 4) device identity, system identifier and location; 5) network addresses and protocols.
Configuration	Review a sample of systems and applications configurations to verify they are set to log all the information specified within the logging policy.
Observation	Observe the production of log events consistently with the system's and application's configuration
Testing Procedure	**Events to be logged**
Interview	

Document	Analyse logging policy to verify they require logging a set of events consistent with applicable requirements, including: 1) successful and rejected system access attempts; 2) successful and rejected data and other resource access attempts; 3) changes to system configuration; 4) use of privileges; 5) use of utility programs and applications; 6) files accessed and the type of access, including deletion of important data files; 7) alarms raised by the access control system; 8) activation and de-activation of security systems; 9) creation, modification or deletion of identities; 10) transactions executed by users in applications.
Configuration	Review a sample of systems and applications configurations to verify they are set to log all the events specified within the logging policy.
Observation	Observe the production of log events consistently with the system's and application's configuration
Testing Procedure	**Unauthorized log change protection**
Interview	
Document	
Configuration	Review a sample of log files settings to verify that users aren't allowed to delete or modify logs and, if they are, those activities are recorded elsewhere
Observation	
Testing Procedure	**Log integrity protection**
Interview	
Document	
Configuration	Review integrity protection mechanisms settings to ensure they operate properly and can't be circumvented
Observation	Observe the production of logs and related integrity protection measures to be operating consistently with their configuration
Testing Procedure	**Log retention**
Interview	
Document	Analyse the logging policy to verify for how much time logs have to be retained.
Configuration	
Observation	Observe log repositories and verify that log retention time is respected and secure deletion is performed thereinafter.
Testing Procedure	**Log analysis**
Interview	Interview responsible personnel to verify how log analysis is performed, how frequently, by what competent personnel and which monitoring activities support the analysis
Document	Analyse the procedures adopted to analyse logs and verify they include: -definition of anomalous behaviours and exceptions -threat intelligence -pattern analysis -monitoring activities support
Configuration	
Observation	Observe a sample of log analysis records to verify they are coherent with the procedures, they are periodically executed and that produced reports can be used for incident management purposes.
ID	**8.20**
Testing Procedure	**Network diagrams**
Interview	
Document	Analyse network diagrams to verify they are current and complete
Configuration	Review network device configuration files to verify network diagrams are correct
Observation	

Testing Procedure	**Authentication systems**
Interview	
Document	
Configuration	Review network device configurations to verify authentication is required
Observation	Observe authentication attempts performed on network devices to verify it is required
Testing Procedure	**Hardening**
Interview	
Document	Analyse network device hardening documentation to verify it is actual, covers all network devices models and mandates disabling of vulnerable network protocols
Configuration	Review network device configurations to verify security hardening measures are consistently applied
Observation	
Testing Procedure	**Network filtering and restriction**
Interview	
Document	Analyse network diagrams to verify network filtering devices are deployed on the boundaries of the network
Configuration	Review network device configurations to verify network filtering devices are configured to restrict and filter inbound and outbound traffic
Observation	
Testing Procedure	**Separate network for the administrator**
Interview	
Document	
Configuration	Review network devices configurations to verify dedicated networks or channels are defined for administration purposes and are segregated from the others
Observation	Observe networks used by the administrators to verify they have a separate address range from other networks and they use a dedicated channel
ID	**8.24**
Testing Procedure	**Cryptography policy definition**
Interview	Interview responsible personnel to verify that topic-specific policy on cryptography is established, communicated to interested parties and that related roles and responsibilities are allocated
Document	Analyse the policy on cryptography to verify that it includes general principles for protection of information, use of cryptography roles and responsibilities and details of all approved algorithms, protocols and keys and key strength
Configuration	Review a sample of cryptography-using systems configurations to verify they are aligned with approved algorithms, protocols and keys and key strength
Observation	
Testing Procedure	**Standards and usage practices compliance with regulations**
Interview	
Document	Analyse the policy on cryptography to verify that approved standards, cryptographic algorithms, solutions and usage practices respect regulations and national restrictions such as: 1) restrictions on import or export of computer hardware and software for performing cryptographic functions or designed to have cryptographic functions added to it 2) restrictions on the usage of cryptography 3) mandatory or discretionary methods of access by the countries' authorities to encrypted information 4) validity of digital signatures, seals and certificates
Configuration	
Observation	
Testing Procedure	**Key management procedures**
Interview	

Document	Analyse procedures for key management to verify they include secure methods for: 1) key generation 2) key distribution 3) key storage 4) key replacement or retirement 5) key destruction
Configuration	
Observation	Review key management logs to verify the documented procedures are followed for: 1) key generation 2) key distribution 3) key storage 4) key replacement or retirement 5) key destruction
Testing Procedure	**Key management logging**
Interview	Interview key management responsible personnel to verify how key management logs are produced and stored.
Document	
Configuration	
Observation	Review key management logs to verify they are produced for every key management related activity, are complete and are retained for a consistent amount of time.
Testing Procedure	**Compromised key**
Interview	Interview responsible personnel to verify that keys are replaced as soon as they are suspected to be compromised
Document	
Configuration	
Observation	Review key management logs to verify suspected compromised keys have been changed
Testing Procedure	**Cryptoperiods**
Interview	Interview responsible personnel to verify that cryptoperiods are defined for all keys based on risk considerations
Document	
Configuration	
Observation	Review key inventories to verify consistent cryptoperiods are defined for all keys
ID	**8.28**
Testing Procedure	**Secure coding governance**
Interview	Interview responsible personnel to verify how organization-wide processes are established and regularly reviewed to provide up-to-date governance for secure coding
Document	
Configuration	
Observation	Observe the practical application of the established secure coding baseline on a sample of actual development projects
Testing Procedure	**Training on secure coding**
Interview	Interview developers to verify they are competent in secure coding techniques and have undergone periodical trainings
Document	
Configuration	
Observation	Review records of training to verify that software developers receive up-to-date training on secure coding techniques periodically, including how to avoid common coding vulnerabilities
Testing Procedure	**Secure design and architecture**
Interview	Interview responsible personnel to verify how secure design and architecture, including threat modelling, is properly performed
Document	
Configuration	

Observation	Review secure design and architecture related records, including threat modelling, to verify they are properly considered before coding
Testing Procedure	**Secure coding guidelines**
Interview	Interview responsible personnel to verify what secure coding practices and techniques are used and documented
Document	Analyse adopted secure coding practices to verify they are adequate to the programming languages and techniques being used
Configuration	
Observation	Review records generated by the application of secure coding practices and techniques to verify they are consistent
Testing Procedure	**Code maintenance**
Interview	Interview responsible personnel to verify that after code has been made operational: 1) updates are securely packaged and deployed 2) reported vulnerabilities are handled 3) errors and suspected attacks are logged 4) external libraries are managed and updated
Document	
Configuration	
Observation	Review a sample of projects to verify they include where applicable: 1) updates of securely packaged and deployed 2) handled reported vulnerabilities 3) logged errors and suspected attacks 4) managed and updated external libraries

ID	**8.32**
Testing Procedure	**Change control procedures**
Interview	Interview responsible personnel to verify that change control procedures are communicated to all interested parties and they are modified as needed
Document	Analyse ICT and software change control procedures to verify they include: 1) evaluation of the impact of changes before authorizing them 2) communicating changes to relevant interested parties 3) tests and acceptance of tests for the changes 4) deployment plans of implemented changes 5) fall-back procedures 6) recording of changes 7) continuity, response and recovery plans 8) operating documentation
Configuration	
Observation	Review a sample of ICT and software change records to verify they always include coherent information about: 1) evaluation of the impact of changes before authorizing them 2) communicating changes to relevant interested parties 3) tests and acceptance of tests for the changes 4) deployment plans of implemented changes 5) fall-back procedures 6) continuity, response and recovery plans 7) operating documentation

Bibliography

[1] Chargebacks911. Chargeback Process. https://chargebacks911.com/chargeback-process/, 2022.

[2] Georg Disterer. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, IV(2):92–100, 2013. doi: doi.org/10.4236/jis.2013.42011.

[3] Fabio Guasconi. Webinar - ISO/IEC 27002-2021 La rivoluzione attesa. Webinar, AENOR Italia, 2021.

[4] ISO. ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. International standard, International Organization for Standardization, Geneva, CH, 2013. URL https://www.iso.org/standard/54534.html.

[5] ISO. ISO 19011 - Guidelines for auditing management systems. International Standard ISO 19011:2018, International Organization for Standardization, Geneva, CH, 2018. URL https://www.iso.org/standard/70017.html.

[6] ISO. ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary. International standard, International Organization for Standardization, Geneva, CH, 2018. URL https://www.iso.org/standard/73906.html.

[7] ISO. ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls. International standard, International Organization for Standardization, Geneva, CH, 2019. URL https://www.iso.org/standard/67397.html.

[8] ISO. *Guidance on the Systematic Review process in ISO*. International Organization for Standardization, Geneva, CH, 2019. URL https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100413.pdf.

[9] ISO. Deliverables: The different types of ISO publications. https://https://www.iso.org/deliverables-all.html, 2019.

[10] ISO. The ISO survey. https://www.iso.org/the-iso-survey.html, 2020.

[11] ISO. ISO/IEC FDIS 27002 - Information security, cybersecurity and privacy protection — Information security controls. 2021.

[12] ISO. ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls. International standard, International Organization for Standardization, Geneva, CH, 2022. URL https://www.iso.org/standard/75652.html.

[13] PCI. Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures . International Standard v3.2.1, Payment Card Industry Security Standards Council, May 2018. URL https://www.pcisecuritystandards.org/document_library?document=pci_dss.

[14] PECB. ISO IEC 27001 Lead Auditor EN v.11.0 Day-1. Distributed for Lead Auditor training course, 2020.

[15] PECB. ISO IEC 27001 Lead Auditor EN v.11.0 Day-2. Distributed for Lead Auditor training course, 2020.

[16] PECB. ISO IEC 27001 Lead Auditor EN v.11.0 Day-3. Distributed for Lead Auditor training course, 2020.

[17] PECB. ISO IEC 27001 Lead Auditor EN v.11.0 Day-4. Distributed for Lead Auditor training course, 2020.

[18] Protiviti. Payment Card Industry Data Security Standard (PCI DSS). https://www.protiviti.com/sites/default/files/united_states/insights/pov-pci-dss-industry-pov.pdf, 2009.

[19] Wikipedia. PDCA. https://en.wikipedia.org/wiki/PDCA, 2022.