Guidelines on assessing DSP and OES compliance to the NISD security requirements

Information Security Audit and Self – Assessment/ Management Frameworks

NOVEMBER 2018

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use ciip&resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

ISBN 978-92-9204-264-6, DOI 10.2824/265743

Table of Contents

Executive Summary 5

1. Introduction 6

1.1 Scope and Objectives 6

1.2 EU Policy Context 7

1.3 Methodology 7

1.4 Target Audience 7

1.5 Document Overview 7

2. Introduction to Information Security Audits 8

2.1 Definition of an IS audit 8

2.2 Forms of an IS audit 8

2.3 Scope of an IS audit 9

2.4 Process of an IS audit 9

2.5 Key outcomes of an audit 10

3. Information Security Audit Lifecycle for NCA 12

3.1 Pre-audit/Planning Phase 12

3.1.1 Scoping 13
3.1.2 Pre-audit issues to consider 13

3.2 Audit Execution/Fieldwork Phase 14

3.2.1 Audit methodology for OES 14
3.2.2 Audit methodology for DSP 23

3.3 Post-audit actions for NCA 27

3.3.1 Post-audit issues to consider 28

4. Mapping to Information Security Risk Assessment/Management Frameworks 30

4.1 Analysis of Relevant (Self) Risk Assessment/Management Frameworks 30

4.1.1 International (Self) Risk Assessment/Management Standards & Frameworks 31
4.1.2 National (Self) Risk Assessment/Management Standards & Frameworks 32
4.1.3 Analysis of Information Security Control Audit Frameworks 33
4.1.4 Mapping Information Security Risk Assessment/Management Frameworks with Information Security Control frameworks. 34

5. Outlook 36

Annex A: Risk Assessment and Risk Management Documentation 37

A.1 Relevant Information Security Control Standards and Frameworks 37

A.1.1 ISO 27001 37
A.1.2 COBIT 5 38
A.1.3 ISA/IEC 62443 39

A.2 Risk Assessment and Risk Management Methodologies and Tools 41

Annex B: International and National (Self) Risk Assessment/Management Standards and Frameworks 54

B.1 International Self-Risk Assessment/Management Standards and Frameworks 54

B.1.1 ISO/IEC 27001 54
B.1.2 OCTAVE 54
B.1.3 CRAMM 55
B.1.4 FAIR 55
B.1.5 IRAM2 55
B.1.6 NIST 800-30 55

B.2 National Self-Risk Assessment/Management Standards and Frameworks 56

B.2.1 BSI-100-3 56
B.2.2 MAGERIT 56
B.2.3 MEHARI 57
B.2.4 MONARC 57

Annex C: Terminology and Abbreviations 58

Executive Summary

According to the NIS Directive[1] Articles 14, 15 and 16, one of the key objectives is to introduce appropriate security measures for operators of essential services (OES) as well as for the digital service providers (DSP) in an effort to achieve a baseline, common level of information security within the European Union (EU) network and information systems. Information security (IS) audits and self–assessment/ management exercises are the two major enablers to achieve this objective.

This report presents the steps of an information security audit process for the OES compliance, as well as of a self-assessment/ management framework for the DSP security against the security requirements set by the NIS Directive. In addition, it provides an analysis of the most relevant information security standards and frameworks to support OES and DSP in practicing the above exercises in the most tailored and efficient manner.

The report identifies numerous parameters towards the successful conduct of information security audits as well as self-assessment/management. Specifically it:

- Proposes an information security audit methodology that could be utilized to facilitate the audit process for OES by the NCA and DSP security self-assessments e;
- Provides an indicative guideline (set of questions) accompanied by evidence that could be utilized to facilitate the overall audit process;
- Proposes to DSP an indicative list of questions, together with relevant evidence, that could facilitate their self assessment exercises against the security requirements prescribed in article 16(1) of the NIS Directive;
- Presents post-audit actions for the NCA with a view to extract benefit and/or knowledge, following an information security audit exercise;
- Illustrates all the information security lifecycle phases and highlights key issues in each phase (e.g. scoping and main challenges during the pre-audit/ planning phase); and
- Presents a comparison of IS audit and self-assessment/management frameworks and methodologies and their correlation with relevant IS audit standards.

Overall, this report is a guidance to national competent authorities in supporting the implementation of the requirements stemming from article 14, 15 and 16 of the Directive.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

1. Introduction

According to the Network and Information Security (NIS) Directive[2] (EU) 2016/1148, Member States should adopt a common set of baseline security requirements to ensure a minimum level of harmonized security measures across EU Member States and enhance the overall level of security of operators providing essential services (OES)[3] and digital service providers (DSP)[4] in the EU. The NIS Directive sets (3) three primary objectives:

- to improve the national information security capabilities of the Member States;
- to build mutual cooperation at EU level; and
- to promote a culture of risk management and incident reporting among actors (OES and DSP) of particular importance for the maintenance of key economic and societal activities in the Union.

This report outlines audit and self-assessment/ management frameworks that can be applied:

- by both OES and DSP regarding the NIS Directive[5] security requirements;
- as the baseline for building an information security program to manage risk and reduce vulnerabilities;
- to define and prioritize the tasks required to enhance security into IT-security risk-based environments.

1.1 Scope and Objectives

The main objective of this report is to facilitate NCA conducting audits and to assist DSP and OES across all EU Member States to comply with the requirements of the NIS Directive in the effort to achieve a baseline security level.

This is achieved by:

a) proposing the information security audit and self-assessment/management frameworks that can be applied by DSP and OES, with regards to the NISD security requirements[6];
b) mapping those frameworks per domain of applicability (i.e. in DSP, OES business environments or both);
c) presenting recommendations to the NCA on how to handle, manage and process the information collected during audits performed on OES.

The key outcome of the study is a set of questions and supporting information that NCA can use to assess OES compliance as well as a set of questions for DSP to perform security self assessments against the NISD security requirements

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[3] ANNEX II of the NISD. According to the NIS Directive 'operator of essential services' means a public or private entity of a type referred in Annex II of the Directive, which meets the criteria laid down in Article 5(2).

[4] ANNEX III of the NIS Directive.

[5] The requirements are defined in Articles 15 and 16 of the NIS Directive.

[6] This objective derives from the fact that there are numerous frameworks developed for specific industries and sectors, incorporating different regulatory compliance goals and varying degrees of complexity and scale. Therefore, the mapping of Information Security Audit and self-assessment/ management Frameworks for DSP and OES should ensure the cultural coverage of both sectorial and cross sectors (e.g. as energy, transport, drinking water and distribution, banking and financial market infrastructures, healthcare and digital infrastructure as referred to in the ANNEX II of the NIS Directive;

1.2 EU Policy Context

The compliance assessment performed by national competent authorities (NCA) is mentioned in articles 14, 15 and 16 of the NISD and defines risk assessment and auditing obligations for the OES and DSP respectively.

- **Article 14:** "Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."
- **Article (15):** "Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide (b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority."
- **Article (16):** "Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: a) the security of systems and facilities, b) incident handling, c) business continuity management, d) monitoring, auditing and testing, and e) compliance with international standards".

1.3 Methodology

This study is based on: (a) desktop research of (inter)national security standards, IS audit frameworks, legislative documents and regulations, good practices and common key policies; (b) an online survey circulated within EU Member States (MS) representatives and experts, including all the identified elements of the desktop research.

1.4 Target Audience

- Operators of Essential Services (OES), either public or private entities, covering a number of sectors as described in Annex II of the NIS Directive[7].
- Digital Service Providers (DSP), any legal entity that provides any digital service, at a distance, by electronic means and at the individual request as described in Directive (EU) 2015/1535[8].
- National Competent Authorities (NCA) on the security of network and information systems, covering the sectors and services referred to in Annex II and Annex III of the NIS Directive.

1.5 Document Overview

The rest of this report is structured as follows:

- Section 2 presents and analyses the forms, the scope, the basic principles, goals, and applicability of Information security audit frameworks for OES and DSP.
- Section 3 provides good practices for NCA and recommendations on performing effective and tailored audits throughout all phases of the audit lifecycle.
- Section 4 provides an overview of relevant information security self-assessment/ management frameworks and alignment to control frameworks .
- Supplementary material regarding the standards and frameworks can be found on Annex A: and Annex B: alongside with terminology and abbreviations on Annex C:.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN

2. Introduction to Information Security Audits

It is common practice to customise an information security standard or framework (based to IT security controls) to fit a particular business environment. Several criteria (e.g. adequacy, sufficiency, validity and acceptability) can be used for this[9, 10]. The "modus operandi" (e.g. form, scope, process, basic principles and goals) of existing information security standards and frameworks are described[11] in the following sub chapters.

2.1 Definition of an IS audit

An information systems security audit is an independent review and examination of system records, activities and related documents. These audits are intended to improve the level of information security, avoid improper information security designs, and optimize the efficiency of the security safeguards and security processes[12].

For the purposes of this document[13] according to articles 14, 15 and 16 of the NIS Directive[14], the primary goals of an IS audit, include (but are not limited to):

- the risk assessment, identification and classification of the organization's information systems and/or assets; and
- the overall evaluation of the organization's design and operating control effectiveness, in all layers, procedural and systemic; and
- the ultimate compliance of all systems and processes of the organization with:
    - the existing regulatory framework (e.g. European and national legislation); and
    - the IT-related policies and standards.

2.2 Forms of an IS audit

There are three main forms of IS audit[15], depending on the relationship between the auditor and the auditee parties:

- **First-party audit** is defined in each and every internal procedure handled by an internal member or group of members within an organisation. The purpose of the first-party audit is to ensure that a process, or set of processes in the quality management system, meets the procedure requirements specified by the enterprise. If the audit is performed by the owner(s) of the process(es) then the audit process is called a self-assessment, which is a commonly accepted procedure of the audit preparation. On behalf of the enterprise, the auditor[16] acts internally and inspects in depth for problematic areas where processes possibly do not comply, and identifies opportunities for improvement.

[9] http://ec.europa.eu/information_society/newsroom/image/document/2018-19/reference_document_security_measures_version_to_be_published_44F171BD-9E21-9945-FB43065BDD852E89_52065.pdf
[10] https://ec.europa.eu/info/law/better-regulation/initiative/167285/attachment/090166e5b833a031_en
[11] Moeller, Robert R. IT audit, control, and security. Vol. 13. John Wiley & Sons, 2010.
[12] https://www.isaca.org/Journal/archives/2016/volume-5/Pages/information-systems-security-audit.aspx
[13] which is to facilitate NCA conducting audits and to assist DSP and OES across all EU Member States to comply with the requirements of the NIS Directive in the effort to achieve a baseline security level.
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[15] http://asq.org/learn-about-quality/auditing/
[16] The auditor acts on behalf of the enterprise rather than a customer or certification body

- **A second-party audit** takes place when the organization performs an audit of a vendor/supplier to ensure that all the requirements specified in the contract between the two parties exists.
- **A third-party audit** occurs when an organization's decision concerns the creation of a quality management system (QMS) that conforms to a standard set of requirements. In this case, an independent company is required to perform an audit to verify and validate the conformity and compliance of the organization with the necessary requirements. These certification bodies conduct audits to compare and verify that the QMS of the enterprise meets all the criteria and requirements of the standard of interest, and continues to meet the requirements on an ongoing basis. Once, the QMS meets the requirements, the certification body approves and delivers the certificate to the organization.

The Directive foresees (article 15 (2b)) that a Competent Authority itself or a qualified auditor might carry out the audit.

2.3 Scope of an IS audit

The scope of an IS audit includes various elements such as the description of the physical locations, the organizational units, the related activities and processes, as well as the timeline needed for conducting the audit. Determining the scope of the audit procedure is the most vital element of the overall audit planning; therefore, the audit scope should be based on, but not limited only to the followings:

- risk exposures, regulatory guidelines and focus to high risk areas as they deserve closer attention and a broader scope to cover all the identified risk factors;
- critical components that directly contribute to recovery capability and operations resilience; and
- the nature of the business operations and the impact on operations of the audit process.

An audit procedure performed by the National Competent Authorities (NCA) should mainly focus on:

- **high risk areas based on national criteria derived from a previously conducted assessment; or**
- **areas that are considered critical, depending on the OES and DSP specialization.**

It has to be noted that the scoping of an audit in the context of the NIS Directive presents several challenges. Section 3.1 provides more information as well as relevant good practices.

2.4 Process of an IS audit

OES as well as DSP should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems, which they use in their operations[17]. Information security risk assessment is the process commonly used to determine these risks and is an integral part and a critical step in the information security risk management process. Risk assessment, even though it is part of the risk management process, is an individual activity (and not a continuous one), initiated when required or at specified regular intervals.

[17] Article 14(1) and 16(1) of the NISD.

Information security risk management can be either implemented individually or it can be part[18] of the overall risk management process[19]. The overall process and structure of an Information Security Risk Management process is depicted in **Figure 1**.

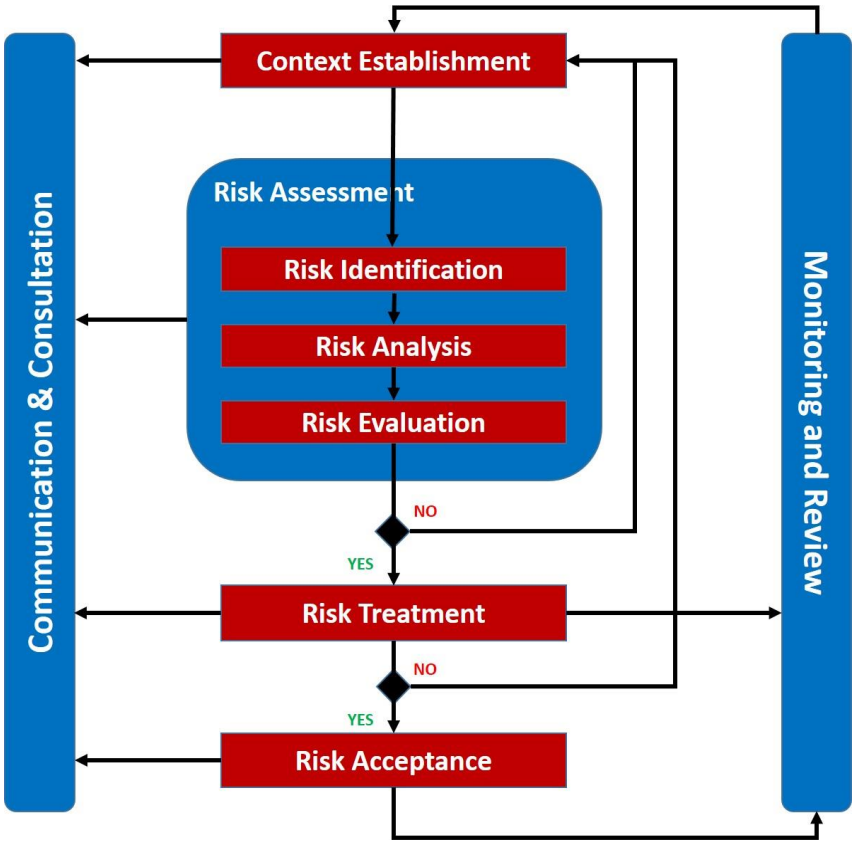

Figure 1. Information security risk management process[20]

The main outcome of a risk assessment process is usually a qualitative, quantitative or a semi-quantitative evaluation of the possible risks that a given system, complex or not, is exposed to, taking into consideration its context and likely threats[21].

2.5 Key outcomes of an audit

One of the primary goals of the audit, is to assess the design and operating effectiveness of the implemented controls on all layers, organizational, procedural and/or technical. An additional key outcome/goal would be the assessment

[18] Risk Management refers to the overall management of risks. IS Risk Management refers to the management of risks derived by IT related risks. Therefore, IS RM can be part of the general RM process.
[19] Technical Department of ENISA Section Risk Management. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools. Technical report, ENISA, 2006.
[20] ISO, ISO, and I. E. C. Std. "ISO 27005: 2011." Information technology–Security techniques–Information security risk management. ISO (2011).
[21] Campbell, T. (2016). "Chapter 14: Secure Systems Development". Practical Information Security Management: A Complete Guide to Planning and Implementation, ISBN 9781484216859.

of the implemented controls' efficiency towards minimizing the identified risk. Finally, the following outcomes, is expected to be achieved during the IS audit lifecycle [22, 23]:

- information and evidence about conformity or non-conformity to all the requirements of the legislative context or/and standards;
- performance monitoring, measuring, reporting and reviewing against key performance objectives and targets;
- auditee management systems and performance regarding the legal compliance;
- review of design and operational effectiveness for all organizational and/or technical controls;
- management responsibility for auditee policies;
- review links between the normative requirements, policy, performance objectives and targets;
- review any applicable legal requirements, responsibilities, competence of personnel; and
- review operations, procedures, performance data and internal audit findings and conclusions.

[22] https://www.iso.org/iso-31000-risk-management.html
[23] https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf

3. Information Security Audit Lifecycle for NCA

The information security audit lifecycle comprises all the steps of the audit process, beginning from the audit planning until the closure of the audit as well as other relevant post-execution actions. **Figure 2** illustrates these phases; a description of each is provided in the following paragraphs.

Figure 2. Information security audit lifecycle for National Competent Authorities

- **Pre-Audit/Planning Phase:** Information needed for the execution of the security assessment is gathered during this phase (e.g. assets to be assessed, main threats against the assets, security controls to be used to mitigate these threats etc.). The security assessment is comprised of a project management plan, specific goals and objectives, scope, requirements, team roles and responsibilities, limitations, assumptions, challenges, timeframe and finally deliverables. All of the above have to be agreed during the planning phase.
- **Audit Execution/Fieldwork Phase:** The execution phase is the main audit phase, during which the intended assessment methodology and technique should be implemented. Upon completion of the execution phase, assessors should have identified system, network and organizational process vulnerabilities.
- **Post-Execution Phase:** This following tasks take place during this phase:
  - analysis of the identified vulnerabilities;
  - root cause identification is performed;
  - recommendations for mitigation measures; and
  - final report drafting.

NCA as well as auditing and certification bodies must focus on all three phases above taking into account the:

- practices and policies of the auditee during normal operation (security and monitoring of systems and facilities);
- practices and policies of the auditee during abnormal operation (incident handling and reporting); and
- compliance with national, international standards and requirements of the NIS Directive.

3.1 Pre-audit/Planning Phase

Prior to the execution of any audit, NCA have to prepare the audit implementation phase, while taking into account numerous factors including but not limited to:

- the nature and scale of the audit;
- the arrangement of assigned resources;
- the understanding of the audit roadmap; and

- challenges and constraints.

3.1.1 Scoping

As part of the pre-audit process[24], a scoping exercise, which ensures compliance with the NIS Directive, must take place. Scoping involves the determination of significant processes, locations (entities) and IT applications and systems that will be subject to assessment. To identify the above as well as their relevant assertions, NCA are required to evaluate[25] the qualitative and quantitative risk factors related to the audited organization. The scoping will have a direct impact on the implementation of controls and the assessment of controls to be performed by the NCA.

More specifically, the first step in scoping, is to conduct an assessment that will enable the NCA to identify the essential services and essential information systems of the auditee. The second step is to perform the risk assessment of the essential services and the underlying infrastructure by taking under consideration numerous factors such as the following:

- the existing processes which support this infrastructure;
- the resilience of systems and services;
- the existing security architecture;
- change and maintenance procedures; and
- past incidents.

According to Annex II of the NIS Directive, there are organizations whose daily activities are based not only on traditional **Information Technology (IT) environments**, but also on **Operational Technology (OT) Environments** (and focus on safety e.g. oil, gas, rail sector,). There are different standards and practices focusing on IT and OT environments, which sometimes create competing priorities. Furthermore, these two areas in many instances do not have the required overarching governance with established communication and/ or cooperation schemes. This separation is evident across many sectors (i.e. transport sector - aviation, maritime, railway), introducing in many instances pitfalls for the audit process and the auditor.

In addition, there are cases where operations of an organization span more than one NIS Directive sector (cross-border and cross-sector) which makes scoping even more challenging.

3.1.2 Pre-audit issues to consider

A big aspect of the pre-audit planning is the timely identification and mitigation of possible challenges during the audit fieldwork. Important factors to consider may include:

- The organization's business model that determines the IT functions' structure and service delivery model (i.e. geographic distribution of IT resources, decentralised IT operations).
- Customization of IT and OT environments increases complexity (architectural diversity) in the risk-assessment management frameworks, requiring a high degree of subject matter expertise during the audit lifecycle.

Additionally, in the context of the NISD audit requirements, the following should be considered:

[24] Although audit is not a requirement for DSP, it is recommended that they take into account similar **scoping considerations** as these presented in this section.
[25] A top-down, risk based approach is recommended in the scoping decisions in accordance with widely accepted information security standards and global best practices.

- Clear definition of the audit universe between the legal (i.e. regulatory issues) basis and the actual audit (compliance): identify the information systems that support the essential service and identify the scope of the audit.
- emerging technology and infrastructure changes: transformation, innovation, disruption;
- pressure of limited skilled resources, budgets and controlling costs: identifying, recruiting and maintaining individuals with the appropriate expertise, managing and controlling costs of the whole procedure;
- audit (and certification) of the supply chain elements/ dependencies: legal obligations differ between OES and DSP, therefore the same audit framework/ security requirements cannot be utilized;
- bridging IT and the business: IT should be integrated and aligned with the business and strategic decisions;
- good practice indicators may differ for each sector and/ or the types of entities that are in the scope of the audit: a baseline is required to ensure a unified control list for auditing all different sectors; and
- sharing the data collected by the audit: sharing of sensitive data should be managed accordingly.

3.2 Audit Execution/Fieldwork Phase

An information Security audit is an assessment of implemented security management controls within an IT system and/or infrastructure and is applicable to both OES and DSP related business environments[26]. The auditing/certification body needs to evaluate (a sample of) the evidence (e.g. computer logs) obtained from the information and operational technology systems of an organization and determine the operational status of the organization (i.e. whether there is evidence that the implemented controls are operating effectively in line with the required level of security assurance). In this context, we suggest three main sources of reference, namely the:

- NIS Directive Cooperation Group security measures for OES[27];
- ENISA report on security measures for DSP[28]; and
- EC implementing act for DSP[29].

The following security measures can be also used by the OES or the DSP as a tool to self-assess the maturity of the practices they follow in combination with well-known capability maturity models (CMM) such as the Capability Maturity Model (CMM®) and Capability Maturity Model Integration (CMMI), or the Business Development Capability Maturity Model (BD-CMM®). In principle, the fundamental concepts of the CMM as a model for optimizing the overall IT (and OT) security audit process can be applied and scaled to enhance any provider in scope of the NISD.

3.2.1 Audit methodology for OES

In this section, a guidance to the NCA on how to facilitate the IS audit for OES is provided. The guidance follows the categorization of the security measures as suggested by the Cooperation Group (see **Figure 3**).

More specifically, the report provides a list of questions categorized per security measure and each question is accompanied by indicative pieces of evidence, which enable the body that performs the audit (as per article 14), to assess whether each control is implemented as intended.

[26] In the case of DSP it will take the form of an internal audit or security self assessment.
[27] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643
[28] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG

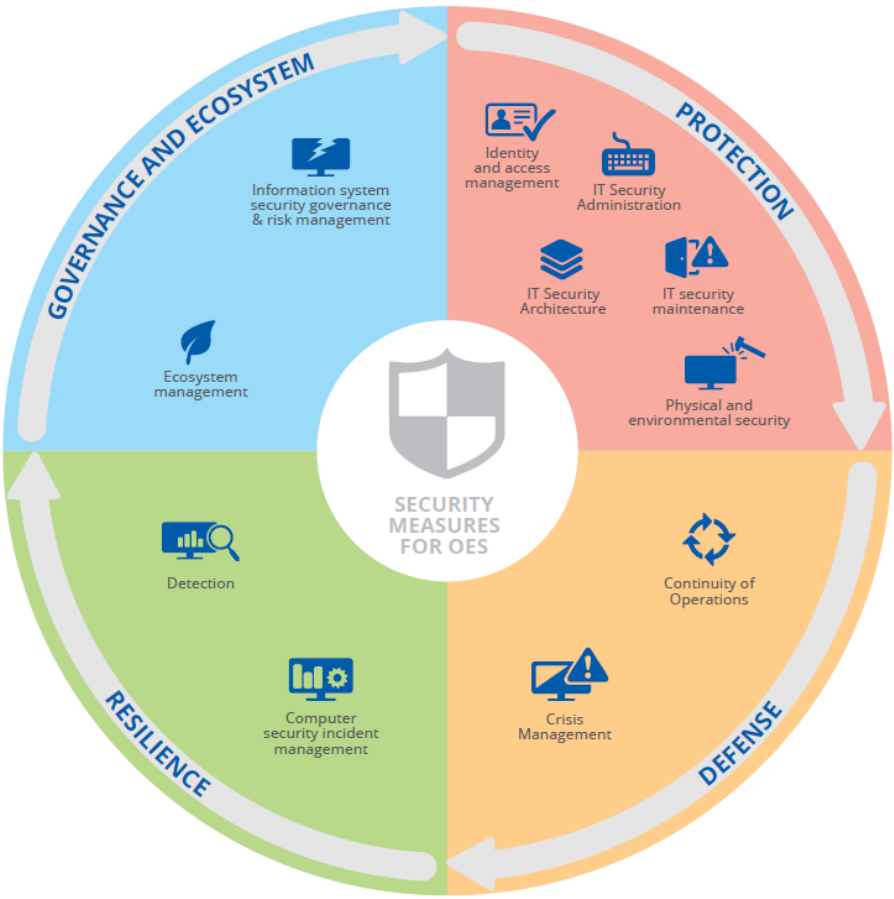

Figure 3. Security Measures for OES

PART 1 – GOVERNANCE AND ECOSYSTEM

1.1 INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MANAGEMENT			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Information System Security Risk Analysis	Is the key personnel aware of the main information security risks and the relevant mitigations?	Evidence of personnel attendance to the training (e.g. accepted invitation, date and agenda of training, signed participation list during the awareness workshop etc.).
		Is there a mechanism for ensuring that all security personnel use the risk management methodology and tools?	Guidance for personnel on assessing risks and list of risks and evidence of updates/reviews documented.
		Is the risk management methodology and/or tools, periodically reviewed, taking into account changes and past incidents?	Documentation of the review process and updates of the risk management methodology and/or tools. Time-table and overall plan of the review cycle.
2	Information System Security Policy	Is there an information security policy (ISSP) and an information security management system (ISMS) in place?	Documented ISS policy in place (dated and signed).

		Are there any certifications in place for specific security risk management standards?	Certification against information security risk management standards (for example ISO 27001), including scope statement.
		Are the information security processes reviewed at regular intervals, while taking into account violations, exceptions and incidents which affected other essential operators/ DSP?	Documentation of review process, taking into account changes and past incidents. Time-table and overall plan of the review cycle.
3	Information System Security Accreditation	Have the systems supporting essential services been regularly subjected to security scans and have they been integrated within the risk management framework of the organization?	Reports from past security scans and security tests.
		Are there policy/procedures in place for the performance of security assessments and security testing?	Documented policy/procedures for security assessments and security testing, which at least include: -which assets should be assessed, -under what circumstances, -the type of security assessments and tests, -frequency, -approved parties (internal or external), -confidentiality levels for assessment and -test results and the objectives security assessments and tests.
		Has the effectiveness of policy/procedures for security testing been evaluated?	List of reports about security assessment and security tests.
4	Information System Security Indicators	Are KPIs implemented in systems supporting essential services to be able to assess their effectiveness at all times?	Documentation of KPIs and mapping with the Critical Information System in which they are implemented.
		Are there any policy/procedures in place for the implementation of security indicators for testing the systems supporting essential services?	Policy/procedures for testing critical information systems, including when tests must be carried out, test plans, test cases, test report templates, desired KPI values.
		Are the aforementioned policy/procedures reviewed and updated?	Updated policy/procedures for testing critical information systems, review comments, and/or change logs.
5	Information System Security Audit	Is there an updated policy and/ or procedure for performing information system security assessments and audits of systems and assets supporting essential services?	Information security audit policy and/ or procedures, formally documented and regularly maintained.
6	Human Resource Security	Are the professional references of key personnel (system administrators, security officers, guards, et cetera) validated?	Documentation of checks of professional references for key personnel.
		Is training material on security issues provided to key personnel?	Evidence of personnel attendance to the training (e.g. Accepted invitation, date and agenda of training,

			signed participation list during the awareness workshop etc.)
		Is key personnel formally appointed in necessary security roles?	• List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles. • Organization's organigram in place, job descriptions signed by key personnel, relevant role trainings attended.
		Are the policies/procedures for the Human Resource security regularly reviewed and updated, taking into account possible changes?	• Comments or change logs of the policy/procedures. • Review time-plan versions of the policies/ procedures providing the changes that took place.
7	Asset Management	Are lists of critical assets and configurations of systems supporting essential services maintained?	Lists of centrally managed critical assets and critical system configurations managed and maintained.
		Is there a policy/procedures in place for asset management configuration control?	Documented policy/procedures for asset management, including roles, responsibilities, assets and configurations that are subject to the policy along with the objectives of the asset management
		Is the asset management policy regularly updated, based on changes and past incidents?	Up to date asset management policy/procedures, review comments and/or change logs.

1.2 ECOSYSTEM MANAGEMENT

S/N	SECURITY MEASURES	QUESTIONS	EVIDENCE
1	Ecosystem Mapping	Are the contract relationships with third parties properly documented and listed?	Lists of all contracts with third-parties
2	Ecosystem Relations	Are the security requirements included in the contracts with third parties?	Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks etc.
		Is a security policy for third parties in place?	Documented security policy for contracts with third parties.
		Is the security policy for third parties reviewed following incidents or changes?	Documented comments or change logs of the policy.
		Are there any residual risks associated to third parties and their services not addressed/mitigated?	• Vendor Risk Assessment/ Management policy/ procedure in place and maintained. • Documented amendment or termination of relationships with high-risk third parties.
		Is a periodic review and update performed to the security policy of third parties, taking into account past incidents, changes, etc.?	Documentation of review process of the ecosystem relations policy.

PART 2 – PROTECTION

2.1 IT SECURITY ARCHITECTURE			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Systems Configuration	Are networks and systems supporting essential services configured with information security in mind?	• System configuration policy and/ or procedure in place and maintained. • System configuration tables. • Timetable and plan of system configuration review cycles.
		Is the effectiveness of the security configurations to protect the integrity of systems evaluated and reviewed?	• Documented past exercises/ tests of critical information systems in place. • Timetable and plan of security configuration reviews.
2	System Segregation	Are the information systems properly segregated in order minimize the potential consequences when risks occur?	Documentation about how the system segregation of CISs and data is implemented.
3	Traffic Filtering	Is there a monitoring mechanism of the systems supporting essential services in place?	Monitoring reports of critical network and information systems.
		Is there a traffic monitoring policy of the systems supporting essential services in place?	Documented policy for monitoring procedures, including minimum monitoring requirements.
		Are there tools in place for supporting the traffic monitoring of the systems supporting essential services?	Proof of existing tools for monitoring systems.
4	Cryptography	Are there cryptographic mechanisms in place to protect the confidentiality and integrity of information stored in or out of the company boundaries (digital facilities)?	Appropriate cryptographic processes exist.
		Are there implemented cryptographic mechanisms such as digital signatures and hashes to detect unauthorized changes to critical data at rest?	Safeguards to protect the secrecy of secret (private) key(s) are in place.

2.2 IT SECURITY ADMINISTRATION			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Administration Accounts	Does the operator set up specific administration accounts, to be used only for administrators that are carrying out specific operations (e.g. installation, configuration, management, maintenance, etc.) on the systems supporting essential services?	Tailored and documented administration accounts with specific access rights given to the relevant personnel.

		Are the administrator accounts solely used to connect to administration information systems?	• Documented management of administrator accounts process. • Logs of administrator account activity available.
2	Administration Information Systems	Are hardware and software resources, used for administration purposes?	Detailed inventory with hardware and software resources used for administration purposes.
		Are administration information systems solely used for administration purposes and not mixed up with other operations?	Administration information systems isolated and segregated from the rest of the infrastructure for enhanced resilience.
		Are the aforementioned resources managed and configured by an authorised operator?	Responsible specialized personnel for the management and configuration of the aforementioned resources.

2.3 IDENTITY AND ACCESS MANAGEMENT

S/N	SECURITY MEASURES	QUESTIONS	EVIDENCE
1	Authentication and Identification	Are there any access control mechanisms in place, for network and information systems, to allow only authorized use?	Access control policy including description of roles, groups, access rights, procedures for granting and revoking the right to access the information systems.
		Are unused or no longer needed accounts deactivated?	Rule definition for deleting no longer used accounts after a short period of time.
		Is there a mechanism in place for monitoring access to network and information systems and for approving exceptions and registering access violations?	Access control related matrices (e.g. segregation of duties control matrix, remote access control, etc.)
2	Access Rights	Are access rights granted in a structured and monitored manner? Are they granted automatically when applicable?	Access right section included in access control policy/ procedures.
		Does the operator define access rights to the multiple functionalities of the resource?	Access rights mapping register to relevant resources and/or processes included in access control policy.

2.4 IT SECURITY MAINTENANCE

S/N	SECURITY MEASURES	QUESTIONS	EVIDENCE
1	IT Security Maintenance Procedure	Has a procedure been established for security maintenance in accordance with the security policy?	Maintenance security procedure properly documented and approved by senior management.
		Are the conditions for enabling the minimum security level for systems supporting essential services resources defined?	Clearly defined minimum security maintenance process.
		Are software and hardware resources regularly maintained and updated?	• Formally documented software and hardware requirements for ensuring compatibility. • Software/ hardware asset management formally documented and maintained.

2	Industrial Control Systems	Considering that the proper operation of many essential services depend on functioning and secure industrial control systems (ICS), does the operator, if applicable, take the particular security requirements for ICS into account?	Formally documented ICS requirements

2.5 PHYSICAL AND ENVIRONMENTAL SECURITY			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Physical and Environmental Security	Is unauthorized physical access to facilities and infrastructure prevented and have environmental controls, for the protection against unauthorized access (such as burglary, fire, flooding, etc.) been implemented?	Basic implementation of physical security measures and environmental controls, such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, CCTVs, etc.
		Has only a limited number of authorized personnel with authorized access and appropriate authorization credentials access to premises containing information systems?	List of personnel with authorized access and authorization credentials.
		Is there a policy for physical and environmental security measures implemented?	Documented policy for physical security measures and environmental controls, including description of facilities and systems in scope.

PART 3 – DEFENCE

3.1 DETECTION			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Detection	Is there a policy and related procedures for incident detection and analysis in place?	Documented incident detection and analysis policy, addressing purpose, scope, roles and responsibilities and coordination among all related entities, including clients.
		Is there a mechanism to ensure that the personnel is available and properly trained to detect, understand and report a security incident?	Reports from related awareness and training exercises.
2	Logging	Is there a mechanism in place for tracking and documenting information security incidents through an incident monitoring process?	Inventory of major past incidents detected and escalated, including all related information (cause, impact, order of actions taken).
		Have the systems been configured in a way that the automatically registering and escalating of incidents, to the appropriate people, is possible?	Systems, tools and procedures for Incident detection and analysis.

3	Logs Correlation and Analysis	Are the information security incidents investigated and are the relevant reports addressed to the organization's management created?	Up to date documentation of the incident detection policy and related procedures and systems
		Is the policy along with the procedures, related to incident detection, updated in regular intervals?	Evidence of reviews of the incident detection policy and the related procedures and systems.
		Do you conduct information security exercises?	Evidence of past related cyber exercises conducted, including the dates they were conducted.

3.2 COMPUTER SECURITY INCIDENT MANAGEMENT

S/N	SECURITY MEASURES	QUESTIONS	EVIDENCE
1	Information System Security Incident Response	Is there a policy, along with related processes or systems, in place for incident response?	Documented incident detection and analysis policy, addressing purpose, scope, roles and responsibilities and coordination among all related entities, including clients.
		Is there a mechanism to ensure that the incident response personnel is available and properly trained to manage and handle incidents?	Records of incident response related training sessions to the appropriate personnel.
		Is the incident response policy and procedures reviewed following an incident?	Systems, tools and procedures for Incident detection and analysis.
		Are there any incident handling processes in place in accordance with industry standards and good practices?	Management commitment with the incident response policy, guidelines and procedures.
2	Incident Report	Is there a register of past security incidents in place?	Existence of reports related to the detection and escalation of past security incidents.
		Is the policy and procedures related to incident response reviewed regularly and updated accordingly?	Up to date documentation of the incident detection policy and related procedures and systems
		Are reviews performed to the incident detection policy and to related procedures and systems?	Evidence of reviews of the incident detection policy and the related procedures and systems.
		Does the organization perform cyber exercises in a regular basis?	Evidence of past cyber exercises conducted, including the dates they were conducted.
3	Communication with Competent Authorities and CSIRTs	Does the operator implement a service that enables it to take note, without undue delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings?	Evidence of communication logs with NCA and/ or CSIRTs.

PART 4 – RESILIENCE

4.1 CONTINUITY OF OPERATIONS			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Business Continuity Management	Has a business continuity strategy for the critical services provided by the organization been implemented?	Formally documented service continuity strategy, including recovery time objectives for key services and processes.
		Are contingency plans for the systems supporting essential services implemented in the organization?	Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives.
		Are all personnel involved in the continuity operations properly trained in their roles and responsibilities with regards to the information system?	Records of individual training activities as well as post-exercise reports.
2	Disaster Recovery Management	Is the organization prepared for recovery and restoration of the services affected by following disasters?	Measures in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, etc.
		Is there a policy in place along with related procedures for deploying disaster recovery capabilities?	Formally documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third par-ties).
		Is all the personnel involved in the disaster recovery operations?	Records of individual training activities.

4.2 CRISIS MANAGEMENT			
S/N	**SECURITY MEASURES**	**QUESTIONS**	**EVIDENCE**
1	Crisis Management Organization	Is there a crisis management policy in place for managing and responding to IT security incidents?	Formally documented crisis management policy which shall at least include critical CIS, information assets, roles and responsibilities in the event of an IT security incident.
2	Crisis Management Process	Does the operator define in its security policy the processes for crisis management which the organization will implement in case of IT security incidents?	Formally documented crisis management procedure

3.2.2 Audit methodology for DSP

According to the NISD, DSPs have to take appropriate and proportionate technical and organisational measures to manage the risk posed to the security of their network and information systems.

Security measures shall ensure a homogenized level of security of network and information systems appropriate to the risk posed for DSP across the Union. According to Article 16(a) of the NIS Directive and its implementation act[30], the security of DSP network and information systems and of their physical environment shall include the following elements (Error! Reference source not found.):

a) security of systems and facilities: Meaning the security of network and information systems and of their physical environment, indicatively including measures such as the systematic management of network and information systems, the physical and environmental security, the security of suppliers and the access controls to network and information systems;
b) incident handling: As far as incident handling, the measures taken by the digital service providers shall include:
    i. detection processes and procedures maintained and tested;
    ii. processes and policies on reporting incidents;
    iii. an incident response process in accordance with established procedures; and
    iv. an assessment of the incident's severity, as well as collection and analysis of relevant information which may serve as evidence and support a continuous improvement process.
c) business continuity management: Meaning the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident;
d) monitoring, auditing and testing: Meaning the appropriate measures, including the establishment and maintenance of policies on:
    i. the conducting of a planned sequence of observations to assess whether information systems maintain functionality as originally intended;
    ii. the inspection and verification to check whether a standard or set of guidelines is being followed; and
    iii. the process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended.
e) compliance with international standards: Meaning, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

[30] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.026.01.0048.01.ENG.

Figure 4 NISD security elements for DSP

ENISA has already published a report[31] with recommended security measures for DSP. The report categorizes measures, into security objectives with the aim to cover all information security domains and provides examples of implementation.

The NIS Directive does not strictly dictate that NCA perform audits of DSP. Furthermore, DSP remain free to take technical and organisational measures they consider appropriate and proportionate to manage the risk. However, it is highly recommended that DSP are prepared to provide NCA with the appropriate evidence of the effective implementation of the required security elements as described above.

To facilitate the audit process, **Table 1** below presents a mapping of the five (5) elements dictated by the European Commission against the relevant (based on the EC Implementing Act) security measures suggested by ENISA. It also includes a list of questions per security measure and each question is accompanied by indicative pieces of evidence, which facilitate the NCA performing the audit.

IMPLEMENTING REGULATION ELEMENTS	SECURITY MEASURE[32]	QUESTIONS	EVIDENCE
Security of Systems and facilities	Physical and Environmental Security	Are there policies and measures for physical and environmental security of datacentres?	Basic implementation of physical security measures and environmental controls, such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, CCTVs, etc.
	Access Control to Network and Information Systems	Are appropriate policies and measures for access to business resources being established and maintained?	• Access logs show unique identifiers for users and systems when granted or denied access.

[31] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/
[32] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

			• Overview of authentication and access control methods for systems and users.
	Integrity of network components and information systems	Is the integrity of the network, platforms and services being established, protected and maintained?	• Software and data in network and information systems is protected using prevention, input controls, firewalls, encryption and signing. • Documentation about how the protection of software and data in network and information system is implemented.
	Change Management	Does change management procedures exist for key network and information systems?	Documentation of change management procedures for critical systems.
	Asset Management	Does asset management procedures and configurations, for key network and information systems, exist?	• An asset inventory or inventories, containing critical assets, their owners and the dependency between assets. • A configuration control inventory or inventories, containing configurations of critical systems.
	Security of Data at Rest	Are there appropriate mechanisms, for the protection of the data at rest, being established and maintained?	• The access control, sharing, copying, transmittal and distribution of confidential and restricted data are defined. • Data retention policy exists and is complete.
Incident Handling	Security incident detection & Response	Are there procedures for detecting and responding to security incidents appropriately?	• Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, security helpdesk for personnel and customers, reports and advisories from Computer Emergency Response Teams (CERTs), tools to spot anomalies, etc. • Inventory of major incidents and per incident, impact, cause, actions taken, and lessons learnt.
	Security incident reporting[33]	Are there appropriate procedures for reporting and communicating about security incidents?	Documented policy and procedures for communicating and reporting about incidents, describing reasons/ motivations for communicating or reporting (business reasons, legal reasons etc.), the type of incidents in scope, the required content of communications, notifications or reports, the channels to be used, and the roles responsible for communicating, notifying and reporting.

[33] This security objective is also present at 'Business Continuity Management' as per the documentation of procedures for internal and external communications in the event of a disruption using a crisis communication plan.

Business Continuity Management	Business continuity	Are there contingency plans and continuity strategy for ensuring continuity of the services offered?	Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives.
	Disaster recovery capabilities[34]	Is there an appropriate disaster recovery capability for restoring the offered services in a case of natural and/or major disasters?	Measures are in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, etc.
	Security of Supporting Utilities	Are there appropriate measures to ensure security of supporting utilities (e.g. electricity?)	Documented policy to protect critical supplies such as electrical power, fuel, etc., describing different types of supplies, and the security measures protecting the supplies.
Monitoring, Auditing and Testing	Monitoring and logging	Are there procedures and systems for monitoring and logging of the offered services?	Security of supplies is protected in a basic way, for example, backup power and/ or backup fuel is available.
	System tests	Are there procedures for testing key network and information systems underpinning the offered services?	• Policy/ procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates. Test reports of the network and information systems, including tests after big changes or the introduction of new systems.
	Security assessments	Are there procedures for performing security assessments of assets supporting digital services?	• Documented policy/ procedures for security assessments and security testing. • Reports from past security scans and security tests.
	Interface Security	Is there a policy for ensuring secure interfaces?	• Formally documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives.
	Software Security	Is there a policy for secure software development?	• Formally documented policy and guidelines, to ensure that software security is maintained. • Evidence of the test results to secure development environments, including measures for protecting test data are maintained.
	Customer Monitoring and log access	Is there a policy which ensures that the software is developed in a manner which respects security?	Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring customer data and logs.

[34] This security objective is also present at 'Monitoring, Auditing and Testing' as per the establishment and maintenance of policies for testing and exercising backups and contingency plans, where needed in collaboration with third parties.

Compliance with (Inter)national Standards	Compliance	Does a policy for checking and enforcing compliance of internal policies against the national and EU legal requirements and industry best practices and standards, exist?	• Updated policy/procedures for compliance and auditing, review comments, and/or change logs. Reports describing the result of compliance monitoring.
	Interoperability and portability	Are any standards which allow customers to interface with other digital services and if needed to migrate to other provides offering similar services?	• State of the art controls exist and are a crucial aspect to mitigate security related risks for customers. • Documentation about how the protection and integrity of infrastructure & virtualization security is maintained.

Table 1. Audit Methodology for DSP

3.3 Post-audit actions for NCA

The results of the audits can be used by the NCA for assessing the security posture not only of a particular operator but also of the sector overall or at a national level. This will assist the NCA in shaping general or sector specific information security policies. Furthermore, the audit output can inform the implementation of the required controls on operational and/ or technical level.

Based on widely accepted good practices, as well as from input of multiple representatives of EU Member States to the Cooperation Group, the following set of post-audit actions are **recommended** to NCA:

- **correlate information security maturity per operator's importance:** The audit outputs in possession of a NCA, can be used to facilitate the creation of a benchmarking dashboard, signifying the information security maturity of OES across the Member State. This dashboard can then be used as a reference point for the assessment of other organizations to be audited by the same NCA and/ or serve as a mechanism for knowledge sharing across NCAs in all EU Member States;

- **provide continual improvement:** The output of an information security audit exercise can also be used to create a baseline required level of security for OES across the jurisdiction of the NCA. The NCA can then use this baseline in order to draft action plans for organizations to monitor their continual improvement towards achieving the required information security baseline level;

- **ensure compliance with information security requirements:** by creating a guideline on how to comply with them;

- **fine tune identification criteria** for OES, in the sense that less 'secure' auditees might take higher priority in the national risk assessment;

As far as the assurance of compliance with information security requirements is concerned, the audit procedure provided in Section 3.2 assures that the monitoring, auditing and testing includes the establishment and maintenance of policies on:

(a) conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;
(b) inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met; and

(c) a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

Data gathered in the above context, shows that the protection of DSP and OES, in some EU Member States, is mainly regulated by specific national acts and methodologies. In some cases though OES and their industry associations may propose their own industry-specific security standards. Furthermore, specific regulations in certain business-sectors may define additional regulations on audits (e.g., regulations on Health, Financial, or Energy sector). The use of the audit output, as derived by the performed analysis, is depicted in the pie chart (**Figure 5**).

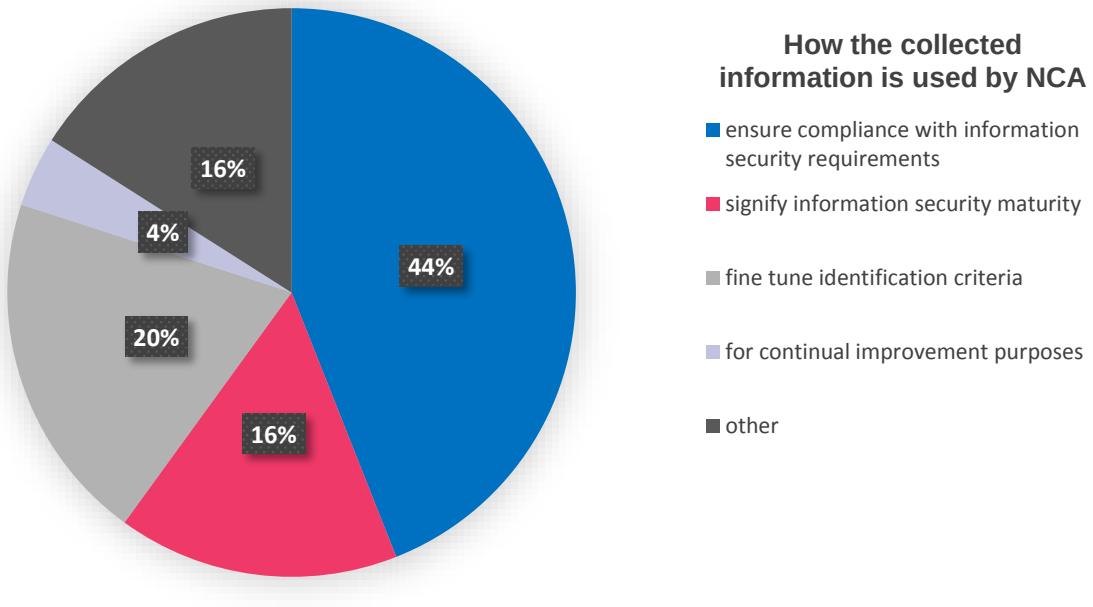

Figure 5. Audit output utilization

3.3.1 Post-audit issues to consider

Evidence Collection Methodologies of NCA

The collection of evidence is a crucial part of any audit. NCA mainly use four ways to collect evidence (in descending order of popularity):

- follow the guidance of a national/ international standard;
- follow the guidance of an underlying framework;
- follow the requirements of a national regulation; and
- base evidence collection on common methodologies/ good practices.

Implementation of Risk-based Information Security approach by MS in the case of DSP

For DSPs, Member States shall ensure that the level of security of NIS is appropriate to the risk posed by **following national and international standards as well as underlying frameworks**, which are selected accordingly in each case. In certain cases, Member States shall proceed with the utilisation of self-assessment methodologies in the case of DSP.

Self risk-assessment provisions of NCA for OES and DSP

In the case of self risk-assessment provisions, the operators and providers are allowed to perform these self-assessments that will be subsequently audited against international standards and/ or sector-specific security standards. National and international standards as well as common methodologies and good practices provide the main guidance and reference point for the risk-assessment exercises conducted by NCA.

Finally, it is important to point out that the establishment and management of a security supervision framework in the context of the NIS Directive, involves several challenges, such as the **lack of resources** and the **rapid change of technology** and standards. Nevertheless, the effective utilisation of the audit output is essential to the evaluation of the implementation of required controls on an operational and/ or technical level.

Implementation Roadmap with corrective actions

The end product of an audit is the report which outlines all observations/ recommendations/ non-conformities depending on the scope and approach of the conducted audit exercise. The audits conducted by the NCA in the context of the NIS Directive should also include an implementation roadmap for the auditee, with proposed corrective actions and an implementation timeframe. The auditee must accept responsibility for the implementation of the aforementioned corrective actions before the agreed timeframe.

4. Mapping to Information Security Risk Assessment/Management Frameworks

Defined OES and DSPs must carefully assess the actual level of preparedness and the related security risks they face in their effort to:

- achieve a minimum, adequate and converged level of security in their networks and information systems (Article 3 of the NIS Directive); and
- implement and establish, monitor, maintain and continuously improve an appropriate level of security.

In the context of auditing, the NCA might decide to follow an already known risk assessment/management framework to ensure compliance of the OES (and possibly DSP) to the requirements of the NISD. In this chapter we present and briefly analyse the most commonly used risk assessment/ management frameworks. We map these against useful criteria for auditing. In Annex A the reader can find more detailed information on these frameworks (tools, plans and methodologies).

4.1 Analysis of Relevant (Self) Risk Assessment/Management Frameworks

Indicative examples of the most widely used and accepted methodologies[35] are listed below:

- ISO/IEC 27001 framework for an ISMS;
- NIST Special Publication 800-30 Rev. 1, Risk Management Guide for Information Technology Systems;
- CRAMM risk management methodology;
- OCTAVE, suite of tools, techniques and methods;
- FAIR, international standards quantitative mode;
- IRAM2, end-to-end approach for performing business-focused information risk assessments;
- BSI 100-3, methodology for performing risk analyses;
- MAGERIT, methodology for Risk Analysis and Management;
- MEHARI, information risk analysis assessment and risk management method; and
- MONARC, risk management methodology.

These methodologies are the most notable in the field of information security for risk assessment and management. For the analysis of the risk assessment/ management methodologies, a set of key criteria was selected:

- **scope/ domain:** defines the scope and the domain of applicability of the methodology;
- **focus (RA/ RM):** defines the focus of the methodology, i.e. risk assessment, risk management or both;
- **control compliance-based:** defines whether the risk is determined through a gap-analysis of the control requirements and the maturity with which they're implemented;
- **flexibility:** refers to the flexibility of the methodology;
- **controlled Scaling:** defines whether the methodology can be scaled to the specific needs of an organization in a centralized, pre-defined way;
- **controlled Tailoring:** defines whether the methodology allows the replacement of specified controls with alternate controls in a centralized, pre-defined way;
- **complexity:** refers to the complexity of the methodology;

[35] For more information regarding the standards, methodologies and tools, please see Annex A:.

- **approach:** refers to the approach of the methodology;
- **assessment Guidance:** defines whether the methodology determines the risk through a gap-analysis of the control requirements and the maturity with which they're implemented;
- **tool Support:** defines whether there is a tool which implements the methodology;
- **supports Third Party Assurance:** defines whether the methodology provides an adequate mechanism for the sharing of reasonably accurate and consistent risk information amongst organizations;
- **year released/ last update:** refers to the release year and the last update of the methodology; and
- **target:** refers to the sector and/ or the types of entities that are in the scope of the methodology.

In the next sub-sections, the methodologies based of these criteria are analysed and categorised into international and national self-assessment/management standards and frameworks.

4.1.1 International (Self) Risk Assessment/Management Standards & Frameworks

The analysis of well-known selected international[36] self-risk assessment/management standards and frameworks based on the aforementioned criteria is presented below (**Table 2**):

S/N	CRITERIA	ISO 27001	OCTAVE	CRAMM	FAIR	IRAM2	NIST 800-30
1	**Scope/ Domain**	SMEs and Large Organizations/ Covers the ISMS of an organization	Large Organizations/ Covers the entire organization	SMEs and Large Organizations/ Covers the IT related risks of an organization	SMEs and Large Organizations/ Covers the entire organization	Large Organizations/ Covers the entire organization	SMEs and Large Organizations/ Covers the IT related risks of an organization
2	**Focus (RA/ RM)**	RA/ RM	RA/ RM	RA	RA	RA/ RM	RM
2.1	Control Compliance-Based	Yes	Yes	Yes	No	Yes	Yes
3	**Flexibility**	Relatively Flexible	Flexible	No Flexibility	Relatively Flexible	Flexible	Relatively Flexible
3.1	Controlled Scaling	Yes	Yes	No	Yes	Yes	Yes
3.2	Controlled Tailoring	Yes	Yes	Yes	Yes	Yes	Yes
4	**Complexity**	Medium Complexity	Low Complexity	High Complexity	Low Complexity	Low Complexity	Low Complexity
5	**Approach**	Asset and control based	Risk-based information security strategic	Qualitative, asset-centric approach	Quantitative approach by filling questionnaire tables	Assessment of risks from a business perspective	Risk-based IT-related risks management

[36] For more information regarding the international standards, please see Annex B:.

			assessment and planning				
5.1	Assessment Guidance	Yes	Yes	No	No	Yes	Yes
6	**Tool Support**	No	Yes	Yes	Yes	Yes	N/A
6.1	Supports Third Party Assurance	No	Yes	No	No	No	No
7	**Year released/ last update**	2005/ 2013	1999/ 2005	1985/ 2011	2001/ 2009	2014/ 2014	2000/ 2012
8	**Target**	All NISD Sectors	All NISD Sectors	All NISD Sectors	All NISD Sectors	All NISD Sectors	All NISD Sectors

Table 2. Criteria for International self-risk assessment/management standards and frameworks

4.1.2 National (Self) Risk Assessment/Management Standards & Frameworks

The analysis of the selected national[37] risk assessment/ management standards and frameworks based on the aforementioned criteria is presented below (**Table 3**)

S/N	CRITERIA	BSI 100-3	MAGERIT	MEHARI	MONARC
1	**Scope**	SMEs and Large Organizations/ Covers the ISMS of an organization	SMEs and Large Organizations/ Covers the entire organization	Medium and Large Organizations/ Covers the entire organization	SMEs and Large Organizations/ Covers the entire organization
2	**Focus (RA/RM)**	RA/ RM	RA	RM	RA, RM
2.1	Control Compliance-Based	Yes	Yes	Yes	Yes
3	**Flexibility**	Relatively Flexible	Relatively Flexible	Relatively Flexible	Relatively Flexible
3.1	Controlled Scaling	Yes	Yes	Yes	Yes
3.2	Controlled Tailoring	Yes	Yes	No	Yes
4	**Complexity**	Medium Complexity	Low Complexity	Low Complexity	Low Complexity
5	**Approach**	Qualitative, Asset and control based	Asset based	Qualitative analysis of risk based on formulas and parameters	Based on risk scenarios for information assets by context and/ or business

[37] For more information regarding the international standards, please see Annex B:.

5.1	Assessment Guidance	Yes	Yes	Yes	Yes
5.2	Integrated Compliance Framework	ISO/IEC 27001	ISO/IEC 13335 ISO/IEC 17799 ISO/IEC 15408 ISO/IEC 27001	ISO/IEC 27001 ISO/IEC 27005 ISO/IEC 13335	ISO/IEC 27000 series
6	**Tool Support**	Yes	Yes	Yes	Yes
6.1	Supports Third Party Assurance	No	No	No	Yes
7	**Year released/ last update**	2004/ 2008	1997/ 2013	1998/ 2010	2016/ 2016
8	**Target**	All	Information and Communication Organizations	Large and Medium Enterprises	All

Table 3. Criteria for International self-risk assessment/management standards and frameworks

4.1.3 Analysis of Information Security Control Audit Frameworks

The information security control standards and frameworks presented above are the most notable[38] in the field of information security. The selected audit frameworks, used in different settings and sectors, are aimed at ensuring that OES and DSPs comply with certain requirements deriving from the NIS Directive.

In this subsection we analyse and categorise the aforementioned standards/ frameworks (**Table 4**) based on the criteria defined below:

- **scope:** the scope of the standard/ framework;
- **software Support:** existence of software which implements the standard/ framework;
- **year released/ last update:** dates of release year and the last update of the standard/ framework;
- **target:** refers to the sector and/ or the types of entities that are in the scope of the standard/ framework;
- **national/ Corporate Level:** refers to the level of applicability of the standard/ framework; and
- **domain of applicability:** operators of essential services or digital service providers or both.

S/N	CRITERIA	ISO/IEC 27001	COBIT 5	ISA/IEC 62443
1	Scope	SMEs and Large Organizations/ Covers the ISMS of an organization	Medium and Large Organizations/ Process-based governance and management of enterprise IT	Medium and Large Organizations/ Covers the entire industrial organization
2	Software Support	No	Yes[39]	No
3	Year released/ Last update	2005/ 2013	1996/ 2013	2007/ 2010
4	Target	All	All	Industrial sector

[38] https://www.enisa.europa.eu/publications/schemes-for-auditing-security-measures
[39] http://www.isaca.org/COBIT/Pages/default.aspx

5	National/ Corporate Level	Both	Both	Both
6	Domain of Applicability/ NISD Sector/ Subsector	All NISD Sectors and Subsectors	All NISD Sectors and Subsectors	Energy, Health sectors and Rail Transport subsector

Table 4. Analysis of selected Information Security Control Standards and Frameworks

The criteria[40] applied in the above analysis allow to highlight the commonalities and differences of the selected audit frameworks. The selected criteria are impartial and unquantifiable, making the comparison of the audit frameworks a straightforward procedure.

As far as the ISO 27001 is concerned, it is an information security standard, not tied to a particular national legislation and it is very popular among security practitioners worldwide. It allows each organization to implement its guidelines in a different manner and select a method that suits its needs. To achieve this it must be used in conjunction with a risk assessment methodology that implements it.

COBIT 5 is a comprehensive framework, which provides a business process-based methodology. It provides a good way of aligning IT and business goals and bridges the gap between business control models and IT control models. Additionally, it provides common language for business executives to communicate with each other on objectives, goals and results.

On the other hand, ISA 62443 is a series of standards, technical reports, and related information that designate processes for applying security measures to organizations in the industrial sector. More information on these standards can be found in Annex A.

4.1.4 Mapping Information Security Risk Assessment/Management Frameworks with Information Security Control frameworks.

Risk assessment/management and information security audit exercises can be directly linked under specific conditions and/or factors. The outcome of a risk assessment/ management exercise could ideally be utilised by an OES, a DSP, an external auditor or even a NCA as input for the conduct of an information security audit.

There are a number of factors that may correlate a risk assessment/ management standard to an information security audit standard (e.g. assessment approach, compliance with International Standards, etc.). This subsection of the report serves the purpose of enabling all stakeholders to proceed following a self-risk assessment to an audit, using the appropriate combination of standards that will provide the required added value to the organization.

Table 5 illustrates a mapping between risk assessment/ management methodologies and audit frameworks, based on specific correlation factors. This mapping indicates risk assessment/ management methodologies, which can provide the input for facilitating the applicable audit procedures.

The research focused on the structure and functionality of the methodologies, i.e. assets or processes, suggests a correlation that leads to better capitalization of risk assessment/ management and audit methodologies. The correlations are indicative and not restrictive.

[40] Macedo, Filipe, and Miguel Mira Da Silva. "Comparative study of information security risk assessment models." Instituto Superior Técnico, UniversidadeTécnica de Lisboa, Lisboa, Portugal (2012).

RISK ASSESSMENT METHODOLOGIES	AUDIT FRAMEWORKS		
	ISO/IEC 27001	COBIT 5	ISA/IEC 62443
ISO/IEC 27001	❶❷	❶❷	❶❷
OCTAVE	❺	❺	-
CRAMM	❶❻	-	❶❻
FAIR	❼	❼	❼
IRAM2	❷	❷	❷
NIST 800-30	❺	-	❺
BSI 100-3	❶❸❻	-	-
MAGERIT	❶❽❾	-	-
MEHARI	❻❽	-	-
MONARC	❹❽	-	-

Table 5. Correlation of Information Security Self Risk Assessment/Management Frameworks with Information Security Control frameworks

Correlation Factors legend

1. Asset based approach	*5. Risk based, IT-related risk management*
2. Process based approach	*6. Qualitative approach*
3. Control based approach	*7. Quantitative approach*
4. Risk scenarios based approach	*8. Compliance with ISO/IEC 27K series*

9. Compliance with ISO/IEC 15408, 17799, 13335

The outcome of the above analysis indicates that specific self-risk assessment/ management methodologies are better combined with specific audit methodologies and procedures. This correlation enables exploiting the advantages derived from each methodology. For example, if the objective is to perform an ISO/IEC 27001 audit, then it is suggested to use a self-risk assessment/ methodology based on the same approach, e.g. asset based approach, or the way of performing the risk assessment or the required detail required for the purposes of the audit, e.g. qualitative or quantitative risk assessment.

These correlations could be utilized by an OES, a DSP, an external auditor or even a NCA as input to the conduct of an information security audit. This analysis enables all stakeholders to proceed following a self-risk assessment to an audit, using the appropriate combination of standards that will provide the required added value to the organization.

5. Outlook

In its entirety, this report aims to provide guidance to the NCA in auditing against the security requirements of the NIS Directive. This report presents the full-fledged set of options for the NCA to meet these provisions. However, the framework to follow lies on the discretion of the NCA. Moreover, this report raises awareness against the most important challenges the NCA will face when auditing and provides some recommendations on how to tackle them.

It is expected that the majority of the Member States will implement their own sectorial security measures. However, we consider this report a common denominator of these approaches as it is based on widely accepted guidance provided by the NIS Cooperation group as well as the EC implementing acts for DSP. In the same line, Member States are expected to follow their own methodologies to assess the security measures of OES and DSP. We consider that the proposed list of questions is a good starting point for the assessment because is based on the most relevant and applicable information security standards.

In addition, the proposed list of questions is outlined with a preventive mode of investigation in mind. Although, all these questions are still valid in the case of a post incident audit, the MS should add additional questions, which address the particularities of the specific incident under investigation.

Each identified framework is different, with its own advantages and disadvantages. The MS has to determine which framework will apply. The optimal choice depends on many factors including the size and maturity of the sector, the resources and skills of the government authority and whether or not there are well-functioning industry initiatives.

Finally, it is worthy to note that the assessment of information security is not a static point-in-time task but a continuous process. The NCA should iterate the evaluation process periodically while taking into account the challenges faced in the previous iterations, the technological changes, the new business scenarios and the new essential services offered.

Annex A: Risk Assessment and Risk Management Documentation

A.1 Relevant Information Security Control Standards and Frameworks

A.1.1 ISO 27001

ISO 27001[41] is an information security standard (Figure 6. ISO 27001 audit framework**Figure 6**), part of the ISO/IEC 27000 family of standards and derived from BS 7799 Part 2, first published by the British Standards Institute in 1999. ISO/IEC 27001 was revised in 2013, bringing it into line with the other ISO management systems standards. It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee.

ISO/IEC 27001 defines the development of an audit programme for the information security management system (ISMS) of the auditee. This programme contains all the relevant information of the audits regarding first-party audits, audits to be performed by clients and third-party audits, as appropriate. The third-party audit procedure is performed by using several checklists:

- audit checklist/ observation form: contains specific items that are particular to the organizational unit to be audited;
- systemic requirements: contains items relating to the requirements of ISO/IEC 27001:2013 and tailored to the auditee specifications each time; and
- control requirements: contains controls depicted in Appendix A of ISO/IEC 27001:2013 and further described ISO/IEC 27002:201342.

ISO/IEC 27001 specifies that once the audit procedure has been completed, the following steps should be taken so as the audit programme is deemed complete:

- review and analysis of findings;
- consolidation of all findings including grouping and tabulation;
- classification of findings;
- preparation of recommendation and audit report;
- classification of findings; and
- preparation of recommendation and audit report.

Whereas the national competent authorities are responsible for identifying non-conformities, OES and DSP are responsible for resolving non-conformities. ISO 27001 provides a taxonomy of possible controls, whereas ISO 27002 provides recommended practices for the implementation of controls. It should be mentioned that ISO 27001 gives auditors a certain degree of freedom, in order to ensure effective and efficient implementation of an ISMS according to the specific information security requirements of the organization under question. Figure 1 below, depicts the overall set-up of ISO 27001 framework.

[41] https://www.iso.org/standard/54534.html
[42] https://www.iso.org/standard/54533.html

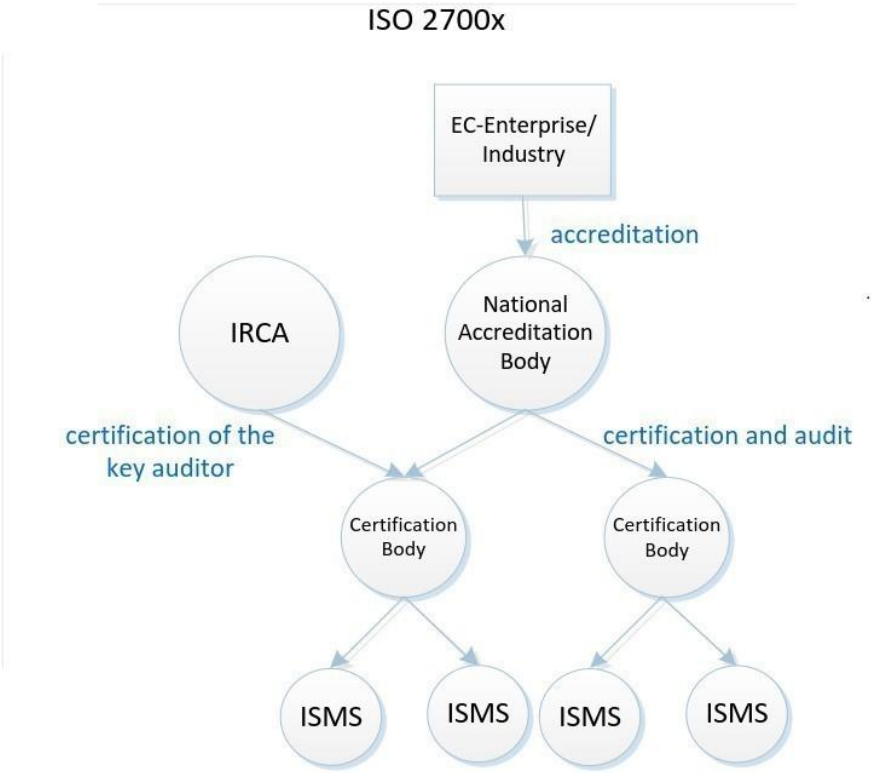

Figure 6. ISO 27001 audit framework[43]

A.1.2 COBIT 5

COBIT 5 (Control Objectives for Information and Related Technology) [44] is a framework aimed to provide an end-to-end business view of the governance of enterprise IT, developed, maintained and distributed by ISACA - Information Systems Audit and Control Association.

COBIT 5 (**Figure 7**) is a comprehensive framework for developing, implementing, monitoring and enhancing information technology governance and management practices by maintaining an equilibrium between realizing benefits and optimizing risk levels and resource use. COBIT 5 provides an effective approach of aligning IT and business goals and bridges the gap between business control models and IT control models while retaining a common language for business executives to communicate with each other about objectives, goals and results. It is based on five key principles for governance and management of enterprise IT. By bringing together those five principles, COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole critical infrastructure, taking in to account the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

Additionally, COBIT 5 aligns with the latest relevant standards and frameworks used by organizations, such as COSO, ISO 31000 and ISO 38500. However, even if COBIT 5 is able to bridge the gap between business control models and IT asset-based RAs, it comes with the disadvantage of utilizing over-complicated concepts and structures that make COBIT difficult and time consuming to apply it as a risk assessment tool.

[43] https://www.enisa.europa.eu/publications/schemes-for-auditing-security-measures
[44] http://www.isaca.org/cobit/pages/default.aspx

As defined in COBIT 5, each phase in the audit process is subsequently divided into key steps to plan, define, perform and report the results of the engagement, as shown in Figure 2 below.

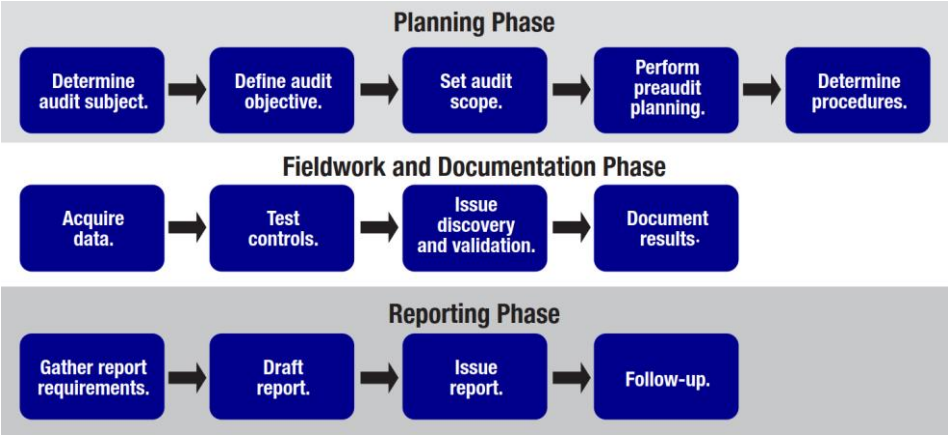

Figure 7. COBIT5 Audit Procedure[45]

A.1.3 ISA/IEC 62443

ISA/IEC 62443[46] is a series of standards, technical reports, and related information that designate processes for applying security measures to industrial zones and is one of the most comprehensive Industrial Automation and Control System Security Standards. This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems. The ISA/IEC-62443 series are organized into four categories, i.e. General, Policies and Procedures, System, and Component[47].

The standards of the ISA/IEC-62443 which are deemed critical for the scope of this research are analysed and depicted in Figure 3, including but not limited to:

- ISA-62443-1-3: System Security Compliance Metrics;
- ISA-62443-2-1: Industrial automation and control system security management system;
- ISA-62443-3-2: (99.03.02) Security for industrial automation and control systems; and
- ISA-62443-3-3: (IEC 62443-3-3) System Security Requirements and Security Assurance Levels.

The ISA/IEC 62443 series of standards propose and introduce the novel concepts of “zones” and “conduits” as a way to divide and segregate the diverse sub-systems in a control system. A zone is designated as a combination of physical or logical assets that share common security requirements related to factors such as consequence and criticality. Additional security measures, such as implementing additional technology or policies, are required if the security level capability of the equipment is deemed no equal to or higher than the requirement level.

ISA/IEC 62443 also provides a framework for industries to achieve and maintain security improvements through a life cycle that integrates design, implementation, monitoring and continuous improvement. The frameworks offers

[45] https://www.isaca.org/COBIT/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.pdf
[46] ISA, Safe and Secure: Multiple Challenges, One Solution, 2014.
[47] ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models: https://www.isa.org/store/products/product-detail/?productId=116720, Accessed on 25/05/2018, 2018.

industrial security solutions and the ability to relevant stakeholders to mitigate information security threats that arise within the segmenting control networks for zones and conduits.

As of today, no ISA/IEC 62443 (**Figure 8**) risk assessment/ management or information security certification exists. ISA is currently working on a modified ISO/IEC 27005 risk assessment/ management process. Furthermore, related audit and evaluation processes are currently being developed, with the goal to provide a way for organizations to assess their current information security posture against the ISA/IEC 62443 family of standards. This assessment will be based on controls mainly deriving from related NIST (e.g. 800-53, 800-60, and 800-70) and FIPS (e.g. 199, 200) publications.

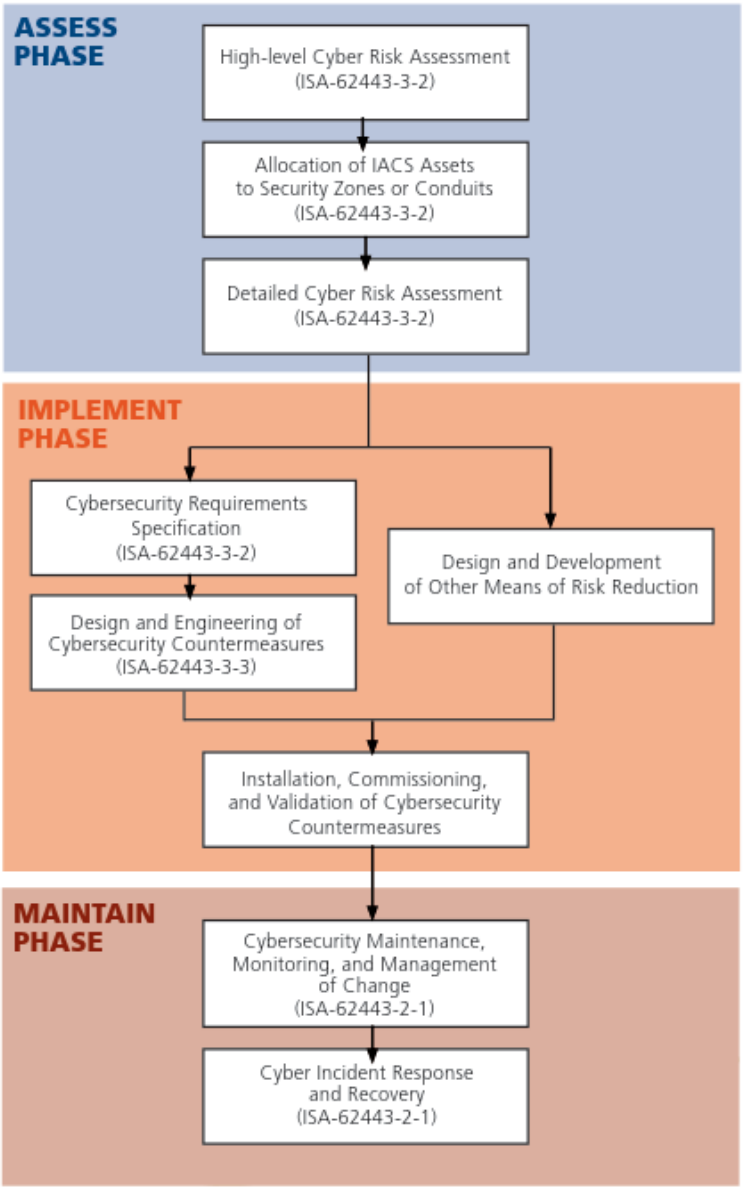

Figure 8. ISA/IEC 62443 Phases

Related information regarding ISA 62443 is not available, as currently no audit/ certification and/ or RA/RM process exists. Currently, and until proprietary ISA 62443 audit standard is published, third-party assurance standards are proposed by ISA. More specifically:

In regards to product assurance

- ISO/ IEC 15408;
- ISO/ IEC 19790 (Similar to NIST FIPS 140-2);
- ISO/ IEC TR/19791.

In regards to Process assurance

- ISO/ IEC 21827;
- ISO/ IEC 17799;
- COBIT5;
- Draft ISA S99 standards, including concepts and process guidance.

In regards to environmental assurance

- ISO 9000 series.

A.2 Risk Assessment and Risk Management Methodologies and Tools

Risk Assessment and Risk Management is the focus of the desktop research. The final results of this research are presented below (**Table 6**). Some key columns in the presented table are the following:

- Target: refers to the sector and/or the types of entities that are in the scope of every document in the table (e.g. federal agencies, ICS, Financial Institutions etc.);
- Country: refers to the country/ies to which the methodology is mainly applied;
- Type: This column refers to the type of documents included in the table (i.e. methodology, standard, guideline, framework, tool);
- Category: distinguishes if document in the table refers to Risk Management, Risk Assessment or to both.

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
1	ISO 27005 - Information technology -- Security techniques -- Information security risk management	The International Organization for Standardization	http://www.iso.org	2011	RM	Standard	International	All
2	ISO 31010 - Risk management -- Risk assessment techniques	The International Organization for Standardization	http://www.iso.org	2009	RA,RM	Standard	International	All
3	ISO 31000 - Risk management -- Principles and guidelines	International Organisation for Standardisation	http://www.iso.org	2018	RM	Standard	International	All
4	COBIT 5	ISACA	https://cobitonline.isaca.org	2012	RM	Framework	International	All
5	Risk IT Framework for Management of IT Related Business Risks	ISACA	http://www.isaca.org	2009	RM	Framework	International	All
6	SARA - Simple to Apply Risk Analysis	Information Security Forum - ISF	http://www.securityforum.org	1993	RA	Method	International	All
7	SPRINT – Simplified Process for Risk IdeNTification	Information Security Forum - ISF European Security Forum	http://www.citicus.com	1997	RA	Method	International	All
8	NIST SP800-30 Guide for Conducting Risk Assessments	NIST	http://nvlpubs.nist.gov	2012/Revision 1	RA	Guideline	USA	All

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
9	NIST SP 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	NIST	http://nvlpubs.nist.gov	2010/Revision 1 (Updated June 2014)	RM	Guideline	USA	All
10	NIST SP 800-39 Managing Information Security Risk Organization, Mission, and Information System View	NIST	http://nvlpubs.nist.gov	2011	RM	Guideline	USA	All
11	MAGERIT	Ministerio de AdministracionesPúblicas (Spanish Ministry for Public Administrations)	https://administracionelectronica.gob.es	2012 v3	RA	Method	Spain	ICT organizations
12	EBIOS	Central Information Systems Security Division (France)	https://www.ssi.gouv.fr	1995 v1 2003 v2	RA, RM	Method and Tool	France	All
13	CRAMM	Central Computer and Telecommunications Agency (CCTA)	-	1987 2003 v5 (the latest)	RA	Method	UK	All
14	BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz	German Federal Office for Information Security (BSI)	https://www.bsi.bund.de	2008/version 2.5	RA, RM	Standard and Method	Germany	All
15	AS/NZS ISO 31000:2009	Standards Australia	https://www.iso.org	2009	RM	Standard	Australia	All

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
	Risk management – Principles and Guidelines							
16	Information Risk Management: HMG IA Standard Numbers 1 & 2	CESG	https://www.ncsc.gov.uk	2015	RM	Standard	UK	All
17	AWWA J100-10(R13) Risk and Resilience Management of Water and Wastewater Systems	American Water Works Association	https://www.awwa.org	2013	RA, RM	Standard	USA	Water
18	Risk Analysis and Management for Critical Asset Protection (RAMCAP) standard for risk and resilience management of water and wastewater systems using the ASME-ITI RAMCAP Plus methodology	ASME Innovative Technologies Institute. American Water Works Association. American National Standards Institute. ebrary, Inc.	https://searchworks.stanford.edu	2012	RA, RM	Standard	USA	Water
19	MIGRA	Selex ES AMTEC / vErlagDatamatS.p.A	http://usa.selex-comms.com	2013	RA, RM	Method and Tool	Italy	Government agencies, large companies
20	ISAMM - Information Security Assessment and Monitoring Method	Telindus N.V. (now acquired by proximus Group)	-	2002	RA	Method	Belgium	All
21	Dutch A&K Analysis	Dutch ministry of internal affairs	n/a	1996 (has not been updated	RA	Method	The Netherlands	

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
				since that time)				
22	Threat Assessment & Remediation Analysis (TARA)	MITRE	https://www.mitre.org	2011	RA	Method	USA	Information Infrastructures
23	Risk Assessment Tools and Practices for Information System Security	Federal Deposit Insurance Corporation	https://www.fdic.gov	1999	RA	Guideline	USA	Finance
24	Microsoft's Security Risk Management Guide	Microsoft	https://technet.microsoft.com	2006/ v1.2	RA	Guideline	International	All
25	Consultation Paper Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)	European Banking Authority (EBA)	https://www.eba.europa.eu	2016	RA	Guideline	Europe	Finance
26	Security Assessment Guidelines for Financial Institutions	SANS	https://www.sans.org	2002	RA	Guideline	USA	Finance
27	Electricity Subsector Informationsecurity Risk Management Process	U.S. Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology (NIST) and the North American	https://energy.gov	2012	RM	Guideline	USA	Energy

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
		Electric Reliability Corporation (NERC)						
28	RVA Model	DEMA	http://brs.dk	2006	RA	Guideline	Danish	All
29	DHM Security Management		http://www.dhm.nl				Netherlands	All sectors of the Dutch critical Infrastructure
30	Good Practice Guide Information Risk Management	National Technical Authority for Information Assurance	http://www.kcgaudit.co.uk	2012	RM	Guideline	United kingdom	All
31	Facilitated Risk Analysis Process (FRAP)	Auerbach Publications	http://www.ittoday.info	2000	RA	Method		All
32	Factor Analysis of Information Risk (FAIR)	RMI Developed by Jack A. Jone	http://www.fairinstitute.org		RA	Framework		All
33	Risk Management Framework (RMF)	NIST	http://csrc.nist.gov	2002	RM	Framework	USA	All
34	Threat, Vulnerability And Risk Assessment (TVRA)	European Telecommunication Standardization Institute (ETSI)	http://www.ttcn-3.org	2009 (basic version) 2010 (advanced version)	RA	Method	Europe	All Also in Transport

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
35	The Overview of IT Security Risk Management: A Lifecycle Approach (ITSG-33)	Communications Security Establishment Canada (CSEC)	https://www.cse-cst.gc.ca	2012	RM	Guideline	Canada	All
36	Good practices for Risk Analysis	NAVI	-	2009			The Netherlands	
37	NRB		https://www.nctv.nl	2007			The Netherlands	
38	European Risk Assessment Methodology project - EURAM	TNO	https://publications.tno.nl	2006-2007	RA	Method	Europe	All
39	CANSO Cyber security and Risk Assessment Guide	CANSO – the Civil Air Navigation Services Organisation	https://www.canso.org	2014	RA, RM	Guideline	CANSO – the Civil Air Navigation Services Organisation – is the global voice of air traffic management worldwide.	Air transport
40	Good Practice Guide - Understand the Business Risk	CPNI	https://scadahacker.com		RM	Guideline	UK	ICS
41	Good Practice Guide - Manage Third Party Risk	CPNI	https://scadahacker.com		RM	Guideline	UK	ICS

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
42	Reducing Operational Risk in Oil and Gas Industry	EMC	https://scadahacker.com	2013	RM	Guideline	USA	Oil & Gas
43	OCTAVE	Carnegie Mellon University Software Engineering Institut	https://resources.sei.cmu.edu	1999/ Version 1.0	RA,RM	Method	USA	Large organizations
44	Octave-S	Carnegie Mellon University, SEI (Software Engineering Institute)	http://resources.sei.cmu.edu	2003 v 0.9 2005 v1.0	RA,RM	Method	USA	Small and medium organizations (with 100 people or less)
45	Octave Allegro	Carnegie Mellon University, SEI (Software Engineering Institute)	http://resources.sei.cmu.edu	2007 v1.0	RA,RM	Method	USA	All
46	MEHARI	CLUSIF	https://clusif.fr/mehari	1996 2010	RA, RM	Method	France	Big and medium size enterprises
47	Information Risk Analysis Methodologies 2 (IRAM2)	Information Security Forum	https://www.securityforum.org	2014	RA,RM	Method	UK	All
48	COSO – Enterprise Risk Management	Committee of Sponsoring Organisations of the Treadway Commission	https://www.coso.org	2004	RM	Framework	USA	All
49	Guidance on Risk Analysis Requirements under the HIPAA Security Rule	Office for Civil Rights (OCR)	https://www.hhs.gov	2010	RA	Method	USA	health

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
50	HITRUST Common Security Framework 2012	HITRUST Alliance	https://hitrustalliance.net	Version 8.1	RM	Framework	USA	Health
51	BS 31100:2011	British Standards	http://shop.bsigroup.com	2011	RM	Guideline	International	All
52	Risk Management Standard, AIRMIC, ALARM, IRM: 2002	AIRMIC (Association of Insurance and Risk Managers) ALARM (National Forum for risk management in the public sector) IRM (Institute of Risk Management)	https://www.theirm.org	2002	RA, RM	Guideline	International	All
53	FFIEC FIL-81-2005	Federal Deposit Insurance Corporation (FDIC)	https://www.fdic.gov	2005	RM	Guideline	USA	Finance
54	API RP 581	American Petroleum Institute (API)	https://global.ihs.com	2000 (original release) 2016 (3rd version)	RA,RM	Method	International	Oil & Gas
55	ANSI/API STD 780	American Petroleum Institute (API)	https://global.ihs.com	2013 (1st edition)	RA	Method	International	Petroleum and Petrochemical Industries
56	ISO/IEC 15408	The International Organization for Standardization	https://www.iso.org	2009 (3nd edition)	RA,RM	Standard	International	All

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
57	MONARC	Cyber world Awareness and Security Enhancement Services (CASES)	https://www.cases.lu	2016	RA,RM	Method	Luxembourg	All
58	NHS Information Risk Management	NHS Digital	http://www.southernhealth.nhs.uk	2015	RA,RM	Framework	UK	Health
59	Cyber security supply chain risk analysis	Shell and Tennet	https://www.cybersecurityraad.nl	2015	RM	Method	The Netherlands	Energy
60	National Risk Assessment	Finnish Ministry of the Interior	http://julkaisut.valtioneuvosto.fi	2016	RA	Method	Finland	All
61	Security Risk Assessment Methodology	Gas Infrastructure Europe (GIE)	http://www.gie.eu	2014	RA, RM	Method	International	Gas
62	EAR/PILAR	EAR/PILAR has been partly funded by the Centro Criptológico Nacional (Spanish National Security Agency)	http://www.pilar-tools.com	2017/version 5.5	RA, RM	Tool that supports Magerit	Spain	All
63	vsRisk	Vigilant Software	http://www.vigilantsoftware.co.uk	2007	RA	Tool	UK	All
64	COBRA (Consultative, Objective and Bi-functional Risk Analysis)	C & A Systems Security Ltd	http://www.riskworld.net	1991	RA, RM	Tool	UK	All

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
65	Cyber Resilience Review (CRR)	Department of homeland Security	https://www.us-cert.gov	2009 (introduced) 2014 (major revision)	RM	Tool	USA	All
66	Cyber security Tool	American Water Works Association	https://www.awwa.org	2014 v1.0 2017 v2.0	RA/RM	Tool	USA	Water
67	Verinice	SerNet GmbH	https://verinice.com	2016 (version 1.13)	RM	Tool	Germany	All
68	FFIEC Cyber security Assessment Tool	Federal Financial Institutions Examination Council	https://www.ffiec.gov	2015	RA	Tool	USA	Finance
69	CSET – Cyber security Evaluation Tool	Department of Homeland Security (DHS) National Cyber security and Communications Integration Centre (NCCIC)	https://ics-cert.us-cert.gov	Version 8.0	RA	Tool	USA	ICS
70	EBA Risk Assessment Questionnaire	European Banking Authority (EBA)	https://www.eba.europa.eu	2016	RA	Tool	Europe	Finance
71	NSRAM (Network Security Risk	The James Madison University	http://www.jmu.edu	2004	RA	Tool	USA	All

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
	Assessment Modelling)	(JMU) CIPP research team						
72	Cyber Infrastructure Survey Tool (C-IST)	SECIR/Stakeholder Risk Assessment & Mitigation	http://tampabay.issa.org		RA	Tool	USA	All
73	Supply Chain Risk Management Review	SECIR/Stakeholder Risk Assessment & Mitigation	http://tampabay.issa.org		RM	Tool	USA	All
74	ICS-CERT Design Architecture Review (DAR)	NCCIC/ICS-CERT	http://tampabay.issa.org		RA	Tool	USA	All
75	ICS Network Architecture Verification and Validation (NAVV)	NCCIC/ICS-CERT	http://tampabay.issa.org		RA	Tool	USA	All
76	Network Risk and Vulnerability Assessment RVA	NCCIC/NCATS	http://tampabay.issa.org		RA	Tool	USA	All
77	Cyber Hygiene (CH) Evaluation	NCCIC/NCATS	http://tampabay.issa.org		RA	Tool	USA	All
78	Control Compliance Suite(CCS) 11 Risk Manager	Symantec Corporation	https://www.symantec.com		RA/RM	Tool	USA	Data Centres
79	Countermeasures	Alion	http://www.countermeasures.com	January 2006 - v8	RA	Tool	USA	All
80	KRiO	SIGEA Sistemas de Protección de la información	https://www.krio.es	June 2015	RA/RM	Tool	Spain	All
81	Modulo Risk Manager	Modulo Security	http://www.modulo.com	5.0 version –	RM	Tool	Brazil	All

S/N	NAME	ISSUER/VENDOR	LINK	RELEASED /VERSION	CATEGORY (RA,RM)	TYPE (METHOD, STANDARD, GUIDELINE, FRAMEWORK, TOOL)	COUNTRY	TARGET
				August 2007				
82	Riskwatch	RiskWatch	http://www.riskwatch.com	2002 - version 9	RM	Tool	USA	All
83	RM Studio	Stiki – Information Security	https://www.riskmanagementstudio.com	v5.1, May 2016	RM	Tool	Iceland	All
84	Smart Information Security Management System (SISMS)	CYMSOFT BILISIM TEKNOLOJILERI	http://www.cymsoft.com	R1 March 2011	RM	Tool	Turkey	All
85	TRICK Service	itrust consulting s.àr.l.	https://www.itrust.lu		RM	Tool	Luxembourg	All
86	Acuity Stream	ACUITY RISK MANAGEMENT LLP	www.acuityrm.com		RM	Tool	United Kingdom	All

Table 6. Risk Assessment and Risk Management Methodologies and Tools

Annex B: International and National (Self) Risk Assessment/Management Standards and Frameworks

B.1 International Self-Risk Assessment/Management Standards and Frameworks

B.1.1 ISO/IEC 27001

ISO/IEC 27001[48] is the international standard for information security management systems (ISMS). The ISO/IEC 27001 Standard provides a methodology which can assist OES and DSP to achieve all of their regulatory compliance objectives concerning the NIS Directive by implementing specific controls. Controls recommended by ISO/IEC 27001 are not only technological solutions but also cover people and organizational processes. There are 114 controls in Annex A covering the breadth of information security management, including areas such as physical access control, security staff awareness programmes, procedures for monitoring threats and incident management processes.

The risk assessment process established by ISO/IEC 27001 follows the below procedure:

- establish and maintain certain information security risk criteria;
- ensure that repeated risk assessments "produce consistent, valid and comparable results;
- identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system;
- identify the owners of those risks; and
- analyse and evaluate information security risks according to certain criteria.

An ISMS is based on the outcomes of a risk assessment based on the ISO/IEC 27001. OES and DSP will need to produce a set of controls so as to minimize the identified risks resulting from the aforementioned procedure.

B.1.2 OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was developed by the Computer Emergency Response Team within the Software Engineering Institute. The goal of the OCTAVE suite of tools, techniques and methods is to allow "risk-based information security strategic assessment and planning"[49]. OCTAVE gives the opportunity to small teams across business units and IT work together to address the security needs of the organization and face the security challenges. It moves an organization towards an operational risk-based view of security and addresses technology in a business context.

The methodology is divided in three explicit methods. The primary OCTAVE method forms the basis for the OCTAVE foundation of knowledge. OCTAVE-S is intended for small and medium sized organizations. The main difference with the basic method is that the necessary knowledge is assumed to be known in advance by the analysis group, so the first step of collecting knowledge is omitted. Lastly, OCTAVE-Allegro offers a faster but more limited approach that focuses on information assets. This approach covers only four simplified steps: development of risk measurement criteria, creation of profiles for each critical information asset, identification of threats to these assets and finally, analysis of resulting risks in order to develop mitigation approaches.

[48] https://www.iso.org/standard/54534.html
[49] CERT (Computer Emergency Response Team). OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation). http://www.cert.org/resilience/products-services/octave/index.cfm

B.1.3 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) was developed in 1987 by a British government organization, the Central Communication and Telecommunication Agency (CCTA), now renamed into Cabinet Office. CRAMM can be used for all kinds of organizations, but it is especially intended for large organizations, like government bodies and industry[50]. It is in use by NATO and corporations working actively on information security. CRAMM helps in justification of security investments by demonstrating need for action at management level, based on quantifiable results and countermeasures from organization.

CRAMM attempts a qualitative approach that focuses on assets. It provides 10 specific and predefined asset tables which classify the assets in categories. Those tables support identification and valuation of assets[51]. Therefore, each asset can be classified into a specific category, each with a predefined list of known vulnerabilities and threats that can exploit them. After the completion of identification and valuation of the assets, the provided dedicated tool automatically suggests a set of all possible countermeasures. However, the usefulness of the method is largely dependent on the tool which implements it.

B.1.4 FAIR

FAIR (Factor Analysis of Information Risk)[52] is an international standard quantitative model for information security and operational risk and provides (a) a model for understanding, analysing and quantifying information risk in financial terms; and (b) a foundation for developing a robust approach to information risk management.

The FAIR framework defines the necessary building blocks for implementing effective risk management programs. FAIR is an ontology of the factors that contribute to risk and how they affect each other. It is primarily concerned with establishing accurate probabilities for the frequency and magnitude of data loss events.

B.1.5 IRAM2

IRAM2 (Information Risk Assessment Methodology 2)[53] is a complete end-to-end approach for performing business-focused information risk assessments. IRAM2 provides the following:

- simple, practical, yet rigorous risk assessment approach;
- focus on the business perspective;
- extended coverage of risks; and
- engagement with key stakeholders.

IRAM2 is supported by four IRAM2 Assistants, each accompanied by a practitioner guide, that help automate one or more phases of the methodology.

B.1.6 NIST 800-30

NIST Special Publication 800-30[54] is a foundation pillar for developing an effective and adequate risk management program. NIST 800-30 provides both the definitions and the practical guidance required for assessing and mitigating risks identified within IT systems. Additionally, it provides information on the selection of practical and profitable security controls that can be utilized to mitigate risk for the better protection of vital information and

[50] European Network and Information Security Agency. Inventory of risk management/risk assessment methods. http://rm-inv.enisa.europa.eu/methods
[51] S.H. Houmb. Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework. PhD thesis, Norwegian University of Science and Technology, Trondheim, 2007.
[52] https://www.fairinstitute.org/fair-risk-management
[53] https://www.securityforum.org/tool/information-risk-assessment-methodology-iram2/
[54] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

the IT systems that process this information. It is composed by well-defined and sequentially steps in order to achieve the aforementioned goals, as depicted below:

- system characterization followed by thread and vulnerability identification;
- control analysis and likelihood determination;
- impact analysis and risk determination; and
- control recommendations and documentation of the results.

Each of the above steps produces an output which in turn feeds the next step of the chain. With respect to the aforementioned, this methodology moves the organization towards to better managing IT-related risks.

B.2 National Self-Risk Assessment/Management Standards and Frameworks

B.2.1 BSI-100-3

BSI 100-3[55] is a methodology for performing risk analyses to additive an existing IT-Grundschutz security concept. This methodology indicates the way of using the threats listed in the IT-Grundschutz Catalogues [GSK] to carry out a bridged analysis of risks for information processing. The methodology is required to be carried out step by step as follows:

- preparing the threat summary: produce a summary of the threats to which the target objects under review are subject;
- determination of additional threats: for the target objects under review there are, in some circumstances, additional isolated threats over and above those foreseen in the IT-Grundschutz Model that must be taken into consideration;
- threat assessment: check whether the security measures already implemented or at least planned in the security concept provide adequate protection for each target object and threat;
- handling risks: decide on how to deal with the remaining threats;
- consolidation of the security concept: check the implemented security measures for each target object using specific criteria; and
- feedback to the security process: Once the security concept has been consolidated, the security process, as specified in the IT-Grundschutz Methodology, can be resumed.

B.2.2 MAGERIT

MAGERIT[56] (Methodology for Information Systems Risk Analysis and Management) is an open methodology for Risk Analysis and Management, developed by the Spanish Ministry of Public Administrations, offered as a framework and guide to the Public Administration. Given its open nature it is also used outside the Administration. MAGERIT was developed in response to the perception that the government and, in general, the whole society increasingly depends on information technologies, that entail certain risks that must be sensibly managed with proper measures, for achieving its service objectives.

MAGERIT seeks to achieve the following objectives: (1) increase the security awareness of those responsible for information systems, (2) offer a systematic and structured method for analysing risks, (3) help in describing and selecting the appropriate measures and controls for treating the risks and (4) prepare the organization for

[55] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1003.pdf?__blob=publicationFile&v=1

[56] Portuguese Ministry of Public Administration. MAGERIT - version 3.0. Methodology for Information Systems Risk Analysis and Management, volume Book 1 - The Method. MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2014.

evaluation, audit, certification or accreditation processes, as relevant in each case. MAGERIT method has the ability to project the risk assessment process at management, operational and technical levels. It is supported by technical documents describing elements and criteria and provides regulatory compliance and compliance to IT standards, such as ISO/IEC 27001:2005, ISO/IEC 15408:2005, ISO/IEC 17799:2005 and ISO/IEC 13335:2004. Furthermore, MAGERIT can be applied as an independent risk assessment method.

B.2.3 MEHARI

MEHARI[57] (Method for Harmonized Analysis of Risk) is a free, open-source information risk analysis assessment and risk management method, developed, maintained and distributed by CLUSIF - Club de la Sécurité de l'Information Français, the French association of information security professionals. MEHARI method bases its analysis on formulas and parameters. This means that MEHARI can only be used in conjunction with dedicated tools. It provides a complete risk management model, description of modular components and processes. It also provides the means to enable classification of assets, the likelihood of threats and measurement of the vulnerabilities through audit. Additionally, it analyses a generic set of risk situations and provides seriousness levels for each risk scenario. Finally, it allows an optimal selection of corrective actions in order to provide risk treatment and gives additional compliance scoring of the organization to ISO/IEC 27001:2005 controls and the ISMS process.

There is a given compliance of the product with international regulations and with most of ISO information security standards. Furthermore, this method provides several indicators (e.g. Efficiency, Resiliency, Continuity aspects) in order to measure the IS maturity level. However, MEHARI risk assessment and risk management methods require in any case a good knowledge of the business internals and the handling of risk.

B.2.4 MONARC

MONARC[58] uses an iterative method which enables the thorough implementation of risk management. This approach, as recommended by ISO 27005, enables the focusing on critical issues, followed by successive iterations to augment the target or further liquidate it to restrict additional risks and therefore to cover more technical aspects. The advantage of MONARC methodology lies in the capitalisation of risk analyses already performed in similar business contexts. In order to achieve its goals, MONARC consists of four (4) well-defined phases as defined below:

- context establishment: take stock of the context, challenges and priorities of the company or organization that wishes to analyse its risks;
- context modelling: provision of details and formalisation of to the identified assets in a diagram that displays their interdependencies.
- evaluation and treatment of risks: quantification of threats, vulnerabilities and impacts to assess the risks; and
- implementation and monitoring: ongoing management phase with security monitoring and recurring control of security measures.

[57] CLUSIF (Club de la Sécurité de l'Information Français). Mehari 2010: Risk analysis and treatment guide. http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf, 2010.
[58] https://www.cases.lu/monarc.html

Annex C: Terminology and Abbreviations

For brevity reasons the following terms and abbreviations are used throughout the report:

- OES: Operators of Essential Services.
- DSP: Digital Service Providers.
- NCA: National Competent Authority.
- IS: Information Systems.
- CIS: Critical Information Systems.
- EU MS: European Union Member States.
- ISO: International Organization for Standardization.
- NIST: National Institute of Standards and Technology.
- ISA: International Society of Automation.
- IEC: International Electrotechnical Commission.
- ICT: Information and Communication Technologies.

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

TP-04-18-691-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-264-6,
DOI 10.2824/265743