Technical Guidelines for the implementation of minimum security measures for Digital Service Providers

DECEMBER, 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

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 Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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 contacting the authors please use **resilience@enisa.europa.eu**
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

Special thank the experts of the ENISA Cloud Security and Resilience expert group, BSI, ANSSI, Microsoft, Google, VMWare, Palo Alto Networks and cyber security experts from the EU Member States, who provided useful comments and feedback on earlier drafts of this document: https://resilience.enisa.europa.eu/cloud-security-and-resilience

ISBN 978-92-9204-203-5, doi 10.2824/456345

Table of Contents

Executive Summary

Online marketplaces, online search engines and cloud computing services are considered as Digital Service Providers (DSPs) in the context of the recently adopted Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, hereafter referred to as the Network and Information Security (NIS) Directive.

The NIS Directive aims to bring cybersecurity capabilities on the same level of development in all the EU Member States. Its purpose is to ensure that exchange of information and cooperation related to security amongst Member States are efficient, including at the cross-border level[1]. With NIS becoming a requirement, the introduction of specific laws in this area across the European Union will have a significant impact to all industry sectors including those relating to DSP categories.

Many businesses in the Union rely on these DSPs for the provision of their services. Some digital services could be an important resource for their users, including Operators of Essential Services (OES), and as such users might not always have alternatives available. The security, continuity and reliability of the type of digital services referred to in this Directive are of the essence for the smooth functioning of many businesses. A disruption of such a digital service could prevent the provision of other services which depend on it and could consequently have an impact on key economic and societal activities in the Union. Such digital services might therefore be critical for the smooth functioning of businesses that depend on them, for the internal market and cross- border trade across the Union[2].

It is essential for all Member States to make sure that they have minimum capabilities to ensure a high level of NIS in their territory and to improve the functioning of the internal market. Commonly defined security measures can support harmonised security practices across EU Member States and potentially enhance the overall level of NIS in the EU.

Therefore, ENISA has issued this report to assist Member States and DSPs in providing a common approach regarding the security measures for DSPs. Although ENISA has already drafted a set of security objectives in the context of cloud security in 2014[3], this study goes further than that by broadening the scope of its work and by including security objectives for all three categories of digital service providers. This study lists 27 Security Objectives (SOs) for DSPs. In those 27 SOs, security measures that map to the NIS Directive requirements[4] are also included.

This particular initiative has been achieved by examining current information and network security practices for the DSPs across the EU. It has brought light to some important findings that can add to existing security objectives and measures in information technology infrastructures in Europe. It is recommended that stakeholders and responsible parties analyse their information security needs in detail in order to evaluate and adapt each of the security objectives and measures according to their specific business requirements.

[1] https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

[2] Preamble 48, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Cloud certification schemes Meta Framework, ENISA, 2014, available at https://resilience.enisa.europa.eu/cloud-computing-certification .

[4] Namely: (a) the security of systems and facilities, (b)incident handling, (c) business continuity management, (d) monitoring, auditing and testing, (e) compliance with international standards

1. Introduction

1.1 Background

1.1.1 General introduction

The world is becoming increasingly interconnected as industries continue to revolutionize and knowledge continues to be shared. With the advent of digital services, network and information systems and services are becoming highly crucial to the society. Thus, it is imperative that their security and reliability is significantly ensured.

In fact, if security and resilience of networks and information systems are not ensured, this can impede the pursuit of economic activities, lead to financial losses, undermine the confidence or cause major damage to the economy of a country. For example, network and information systems, and primarily the Internet, play an essential role in facilitating the cross–border movement of goods, services and people. Substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. Knowing how to properly address network and information security is key to avoid any damaging effects.

DSPs operate in a fast changing environment and should ensure a level of security proportionate to the degree of risk posed to the digital services they provide. Responsibilities in ensuring the security of network and information systems lie to a great extent with DSPs themselves. A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements, standards and commonly acceptable industry practices.

1.1.2 Objectives

The objectives of this report are to:

- Define common baseline security objectives for Digital Service Providers (DSPs).
- Describe different levels of sophistication in the implementation of security objectives.
- Map the security objectives against well-known industry standards, national frameworks and certification schemes.

1.1.3 Scope & Target Audience

This study analyses the security objectives by providing security measures and examples of implementation concerning the digital service providers and in particular:

- Cloud computing service providers
- Online marketplaces
- Online search engines

The three DSP categories are described in the NIS Directive[5] as follows:

- **Online marketplaces:**

  An online marketplace allows consumers and/or traders to conclude online sales and service contracts with traders, and is the final destination for the conclusion of those contracts. It does not

[5] Preambles (15), (16) and (17) of the NIS Directive

cover online services that serve only as an intermediary to third-party services where a contract can ultimately be concluded. It therefore does not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product. Computing services provided by the online marketplace may include processing of transactions, aggregations of data or profiling of users. Application stores, which operate as online stores enabling the digital distribution of applications or software programmes from third parties, are to be understood as being a type of online marketplace

- **Online search engines:**

  An online search engine should allow the user to perform searches of in principle all websites on the basis of a query on any subject. It may alternatively be focused on websites in a particular language. The definition of an online search engine provided in this Directive should not cover search functions that are limited to the content of a specific website, irrespective of whether the search function is provided by an external search engine. It should also not cover online services that compare the price of particular products or services from different traders, and then redirect the user to the preferred trader to purchase the product.

- **Cloud computing service providers:**

  Cloud computing services span a wide range of activities that can be delivered according to different models. For the purposes of this report, "cloud computing services" means services that enable access to a scalable and elastic pool of shareable computing resources. The term "computing resources" covers resources such as networks, servers or other infrastructure, storage, applications and services. "Scalable" means that, in order to handle fluctuations in demand, computing resources are flexibly allocated by the cloud service provider irrespective of the geographical location of the resources.

The articles 4(17), (18) and (19) of the NIS Directive provide the definitions of the DSPs.

Privacy is of outmost importance for the personal data being processed by DSPs but it is considered out of scope for this particular report. This is because, there is a good deal of data protection requirements (i.e. consent of the data subject, the purpose definition, proportionality of collected data etc.) and tools (i.e. privacy by design, privacy impact assessment, privacy seals, notifications of the processing to and audits by the national Data Protection Authorities (DPAs) and data breach notifications) which are examined under a very specific piece of EU Regulation, the General Data Protection Regulation (GDPR). The identification of the entire set of organisational and technical measures which are deemed adequate to GDPR is a subject for thorough analysis which exceeds the boundaries of the current undertaking. For this reason, this report focuses only on the objectives which are solely considered most relevant to the security element of the information systems and data maintained by the DSPs. However, some security measures described herein i.e. encryption, secure disposal of data, media access policy etc. are extensively used to address data protection requirements as well.

1.1.4 Document overview

The report lists and describes the high-level security objectives for the DSP categories together with the different sophistication levels in the implementation of security measures. For each sophistication level (basic, industry-standard and state of the art), the corresponding measures and examples are provided.

The report also provides a mapping between security objectives, industry standards, certification schemes and national frameworks. The goal of the mapping is to allow DSP communities to understand more easily if their NIS requirements and security objectives meet the requirements of those frameworks.

1.1.5 Methodology

This study is based on the Cloud Certification Schemes Meta framework (CCSM) released in November 2014[6] by ENISA, regarding cloud service providers. This tool is a meta-framework that provides a neutral high-level mapping from the customer's Network and Information Security requirements to security objectives in existing cloud certification schemes.

Additional security objectives concerning cloud services that may have come into play since 2014 have also been examined. The list of objectives has been validated with the ENISA Cloud Expert Group through extra consultation and a validation workshop.

A questionnaire was developed and a publicly available online survey was launched in order to identify several security controls and measures implemented, along with good practices and standards deployed by DSP and in particular online market places and online search engines.

The diagram below illustrates the relationship between **security requirements, security objectives** and **security measures** which are key terminologies that have been used throughout the document. Further to this, examples of these terminologies are also described below.

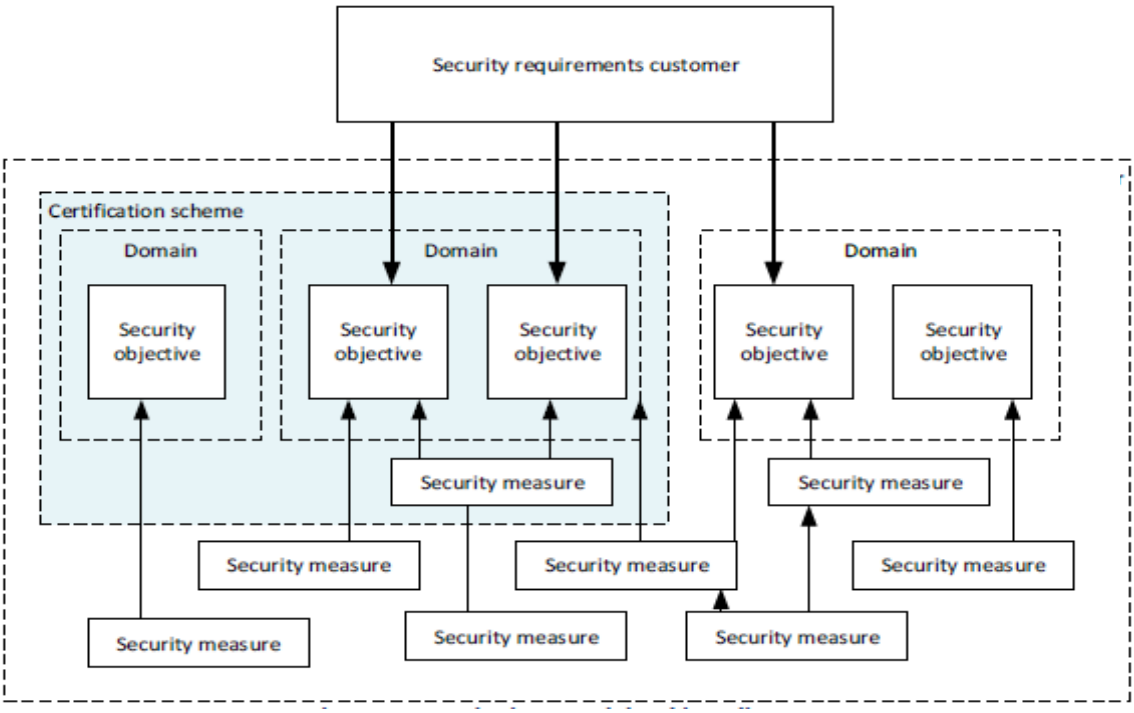

Figure 1: Terminology explained in a diagram extracted from "Cloud Certification Schemes Meta framework"

[6] https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework

- **Security requirement:**

  Customers have security requirements. In the procurement phase customers usually check which security requirements are met by the security objectives of the provider. This process is often referred to as due-diligence.

- **Security objectives:**

  Providers have security objectives. Objectives are high-level goals and usually do not include many technical details. For example, "we offer an uptime of 99.9%", or "customer data cannot be accessed by unauthorized personnel". Security objectives are sometimes grouped in "security domains" (e.g. "software security"). Security objectives are sometimes called "control objectives").

- **Security measures:**

  Providers have security measures in place, to reach the security objectives. Security measures are sometimes called "controls" or "security controls"-.

The report also provides a mapping between security objectives and the following industry standards, certification schemes and national frameworks:

- **ISO/IEC 27001:**2013
- **CSA CCM:** Cloud Controls Matrix v3.0.1
- **BSI C5:** Cloud Computing Compliance Controls Catalogue (C5), criteria to assess the information security of cloud services, version 1.0 – as of February 2016
- **COBIT5:** Framework for the governance and management of enterprise IT
- **CCS CSC:** The CIS Critical Security Controls for Effective Cyber Defence, Version 6.1, August 31, 2016
- **OCF:** CSA STAR PROGRAM & OPEN CERTIFICATION FRAMEWORK IN 2016 AND BEYOND
- **NIST:** Framework for Improving Critical Infrastructure Cybersecurity**,** Version 1.0**,** National Institute of Standards and Technology**,** February 12, 2014
- **PCI DSS:** Payment Card Industry (PCI) Security Standards Council, Data Security Standard Requirements and Security Assessment Procedures, Version 3.2, April 2016
- **CES:** Cyber Essentials Scheme, Requirements for basic technical protection from cyber attacks, June 2014

2. List of security objectives and measures for DSPs

2.1 Description

For each security objective we provide:

- Brief description of the security objective.
- Levels of sophistication on the implementation of security measures with examples.
- A mapping with industry standards, certification schemes and national frameworks

The list below, categorizes security measures into three sophistication levels. Each level contains the practices to assess the adequacy of the design and evidence that should be provided in order to check the effective implementation of the security practice. For each security objective, we have provided security measures that are either basic, industry-standard or state of the art. Readers can refer to the table below for the definition of each of these sophistication levels[7] and can also refer to the list below for an overview of the security levels of each objective.

SOPHISTICATION LEVEL	DESCRIPTION OF SOPHISITICATION LEVELS
1 –Basic	-Basic security measures that could be implemented to reach the security objective -Examples that basic measures are in place
2 – Industry standard	-Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents. -Examples of industry standard measures and evidence of reviews of the implementation reacting to changes and/or incidents.
3 – State of the art	-State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures -Examples of state of the art (advanced) implementation, evidence of a structural review process, and evidence of pro-active steps to improve the implementation of security measures.

Sophistication levels are applied independently to each objective. As a result, a DSP may receive different sophistication ratings for different objectives. It is important to realise that the sophistication levels that are applicable to a given organisation depend on its specific characteristics such as its size or the services provided. For example, for a provider with only 5 employees it may be unnecessary to have a security policy that is fully aligned with best practice industry standards, or to have a documented formal procedure for hiring personnel.

The practices that complete each sophistication level are selected from relevant standards, guidelines and frameworks which have been identified during the stock taking exercise and described in the section 1.1.5.

[7] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

2.2 The role of risk assessment

DSPs wishing to establish, implement, operate, monitor and continuously maintain and improve an appropriate level of security, must also carefully and continuously consider and assess the actual level of preparedness and the related security risks they face.

A risk assessment should be performed throughout the system life cycle: during requirements definition, procurement, control definition and configuration, system operations, and system close-out.

A "Risk Assessment" (RA) would be, in this context, an important step to be performed before deciding the required sophistication levels needed by the DSP. The extent and granularity of the Risk Assessment should take into account several factors such as the size of the organisation, the implementation cost of the measures etc.

The risk assessment allows the DSP to define a threshold for the minimum acceptance level before the establishment of a risk value and to perform the risk assessment for the assets in scope. Therefore, a risk assessment is a key preliminary step that should be conducted in order to understand what risk level is appropriate/acceptable for each organisation before deciding upon the required sophistication levels needed by DSPs.

The organisation should select specific controls, measures and sophistication levels by considering and effectively using the results of the risk assessment. This way, the proposed security measures could be considered as an appropriate benchmark enabling the security managers to determine which specific aspects of security require attention and priority within their respective organisations.

Establishing a security benchmark within a context that has been defined by DSP security experts is considered to be a successful formula, because such a benchmark can be properly focused on DSP specific security issues. Such benchmark can complement the outcome of the risk assessment and provide an additional input for defining and selecting the specific controls, measures and sophistication levels for the security of the services offered by the DSPs.

The above-described proposed approach is aligned with general risk management good practices – and therefore will help create synergies between the risk management and the security efforts of the DSP. In contrast with a compliance based approach, this approach is considered to be more pragmatic and efficient. Moreover, the proposed approach is considered to be more powerful because it takes into consideration the specific characteristics of DSPs. Therefore, it can be applied to a wide range of DSPs independently of their size or maturity.

The use of sophistication levels allows the definition of different quality requirements for each measure. This approach is different from a maturity level approach because, in practice, an organisation will probably not have all its measures developed to the same level of maturity.

The identification of a suitable risk assessment methodology for DSPs is beyond the scope of this report; therefore, it has not been described in detail. Only the relevance and usefulness of performing a suitable risk assessment, before deciding the required sophistication levels, was highlighted (SO 02: Risk Management).

2.3 SO 01 - Information security policy

Description

The DSP establishes and maintains an information security policy. The document details information on main assets and processes, strategic security objectives.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Set a high level security policy, which is aligned with business objectives and addresses the security and continuity of the communication networks[8] and/or services provided. • Make key personnel aware of the security policy.	• Documented security policy, including networks, systems and services in scope, critical assets supporting them, and the security objectives. • Key personnel are aware of the security policy and its objectives (interview).
2	• Set detailed information security policies for critical assets and business processes. • Make all personnel aware of the security policy and what it entails for their work. • Review the security policy following incidents.	• Documented information security policy, approved by management, including applicable laws and regulations, accessible to personnel. • The information security policy is easily accessible to staff. • Personnel are aware of the information security policy and what it implies for their work (interview). • Review comments or change logs for the policy.

3	Review the information security policies periodically, and take into account significant system changes, violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	• Information security policies are up to date and approved by senior management.
		• Logs of policy exceptions, approved by the relevant roles.
		• Documentation of review process, taking into account changes and past incidents.
		  ○ Last planned review has been done according with the review process.
		  ○ Records of the management review.
		  ○ Meeting minutes of review sessions.
		  ○ Feeds and insights collected from internal security solutions and external databases

[8] These security and continuity requirements come from the risk analysis a DSP should perform (SO 02 – Risk Management)

Mapping

ISO27001: A.5 Information Security policies CSA CCM: (GRM-01, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09)

CSA CCM: (GRM-01, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09) Governance and Risk Management

BSI C5: OIS-01, OIS-01H, OIS-02, SA-01, SPN-02, SPN-03

CCS: 5.15 Configuration Management, 5.16 Data Management, 6.1 Location of Data and Data Centers, 6.2 Compliance Management, 6.3 Policy Management, 6.4 Audit Management, 6.12 Security Management

OCF: (GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11) Governance and Risk Management

NIST: ID.GV-1: Organizational information security policy is established

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.1 & 12.1.1

2.4 SO 02 – Risk Management

Description

The DSP establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risks management procedures can include (but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools and Risk Assessment (RA) tools etc.

Security measures in sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Create a list of the main risks for security and continuity of the provided communication networks, systems or services, taking into account the main threats for critical assets. • Consider risks which stem from data protection or other sector-specific regulations or policies into the risk assessments. • Make key personnel aware of the main risks and how they are mitigated.	• List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security, continuity and privacy of networks and services. • Key personnel are aware of the main risks (via interviews, ad hoc tests).
2	• Set up a risk management methodology and/or tools based on industry standards.	• Documented risk management methodology and/or tools which contains, at least: o Objectives, roles, and responsibilities; o Scope of the risk management methodology;

	• Ensure that key personnel use the risk management methodology and tools. • Review the risk assessments following changes, security incidents or data breaches. • Ensure residual risks are accepted by management.	○ Procedures that supports the risk assessment; ○ Catastrophic but improbable events that could affect to the offered services. • Guidance for personnel on assessing risks. • List of risks and evidence of updates/reviews. • Review comments or change logs for risk assessments. • Management approval of residual risks.
3	Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	• Documentation of the review process and updates of the risk management methodology and/or tools. ○ Last planned review has been done according with the review process. ○ Records of the management review. ○ Meeting minutes of review sessions

Mapping

ISO27001: ISO27001:2013 (all)

CSA CCM: CSA CCM (GRM-02, GRM-04, GRM-08, GRM-10, GRM-11, STA-01, STA-04, STA-04, STA-05, STA-06) Governance and Risk Management, Supply Chain Management, Transparency and Accountability

BSI C5: OIS-06, OIS-07, OIS-07H, OIS-03H, SA-01, SA-03, BEI-04, SPN-02, SPN-03

CCS: CCS, 6.2 Compliance Management, 6.3 Policy Management, 6.11 Risk Management, 6.12 Security Management

OCF: OFC, (GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11) Governance and Risk Management, (STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09) Supply Chain Management, Transparency and Accountability

NIST: ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.2

2.5 SO 03 – Security Roles

Description

The DSP assigns appropriate security roles and security responsibilities to designated personnel. (i.e. CSO, CISO, CTO etc.)[9].

[9] This objective might be merged with SO 01: 'Information Security Policy' in case that the DSP decides to include the management of the security policy into the policy itself.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Assign security roles and responsibilities to personnel. • Make sure the security roles are reachable in case of security incidents.	List of security roles (CISO, DPO, business continuity manager, etc.), who occupies them and contact information.
2	• Personnel is formally appointed in security roles • Make personnel aware of the security roles in your organization and when they should be contacted.	• List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles (CISO, DPO, etc.). • Formal appointment of the key security roles and responsibilities. • Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
3	Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	• Up-to-date documentation of the structure of security role assignments and responsibilities. • Documentation of review process, taking into account changes and past incidents.

Mapping

ISO27001: A.6.1 Internal organization

CSA CCM: (BCR-10, CCC-01, DSI-06, GRM-06, HRS-03, HRS-07, IAM-02, IAM-05, IAM-09, IAM-10, SEF-01, SEF-02, SEF-03) Business Continuity Management & Operational Resilience, Change Control & Configuration Management, Data Security & Information Lifecycle Management, Governance and Risk Management, Identity & Access Management, Security Incident Management, E-Discovery & Cloud Forensics

BSI C5: OIS-02, OIS-03, OIS-04, SA-01, BCM-01

CCS: 5.13 User Management and Authentication, 6.5 Data Protection, 6.10 Employee Management

OCF: OCF, (BCR-01, BCR-02, BCR-03,BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11) Business Continuity Management & Operational Resilience, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11,IAM-12,IAM-13 Identity & Access Management, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05 Security Incident Management, E-Discovery & Cloud Forensics

NIST: ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.4

2.6 SO 04 – Third party management

Description

The DSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES

1	• Contractual agreements when dealing with third parties and customers have been established.
	• Include security requirements and relevant tasks in contracts with third-parties and customers.
	• Communicate residual risks which might affect the offered services to the customers.
		• List of relevant third party contracts.
		• List of customer access request.
		• Identify selection criteria.
		• Documented contractual agreements containing at least:
		  ○ Service description;
		  ○ Security measures;
		  ○ Non-disclosure agreements;

LEVEL	SECURITY MEASURES	EXAMPLES
	• Retain the right to perform second party audits where it is deemed necessary from a risk perspective. • Responsibilities regarding the maintenance, operation and ownership of assets have been defined.	○ Roles and responsibilities; ○ Target service levels; ○ Contacts and reporting lines; ○ The right for second party audits. • Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centers, interconnections, shared facilities, et cetera.
2	• Set a security policy for contracts with third-parties. • Ensure that all procurement of services/products from third-parties follows the policy. • Review security policy for third parties, following incidents or changes. • Perform risk analysis before entering any outsourcing agreement. • Mitigate residual risks that are not addressed by the third party.	• Documented security policy for contracts with third parties. • Contracts for third party services contain security requirements, in line with the security policy for procurement. • Review comments or change logs of the policy. • Past risk analysis reports. • Residual risks resulting from dependencies on third parties are listed and mitigated. • Documented third parties' contractual agreements contains special requirements in case of: ○ Major blackouts; ○ Natural catastrophes; ○ Accidents or other possible emergency situations; ○ Blackout resistance.
3	• Keep track of security incidents related to or caused by third-parties. • Periodically review and update policy for third parties and reevaluate outsourcing agreements at regular intervals, taking into account past incidents, changes, etc.	• List of security incidents related to or caused by engagement with third-parties. • Documented results of monitoring activities. • Documented results of auditing activities. • Identify the process(es) applied to manage recent changes and confirm: ○ Adequate warning to all stakeholders is provided; ○ Involves relevant personnel; ○ Includes procedures for backing-out from failed changes.

Mapping

ISO27001: A.15.1 Information security in supplier relationships

CSA CCM: (CCC-02, STA-01, STA-02, STA-03, STA-04, STA-05, STA-05, STA-06, STA-07, STA-08, STA-09) Change Control & Configuration Management and Supply Chain Management, Transparency & Accountability

BSI C5: HR-03H, DLL-01, DLL-02, UP-01, BEI-02

CCS: 6.6 Terms and Conditions of Use, 6.8 Contract Management, 6.13 Embedding External Services, 7.7 Service Level Management

OCF: OFC, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability

NIST: PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.8.3

2.7 SO 05 – Background checks

Description

The DSP performs appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory framework. Background checks may include checking past jobs, checking professional references, etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Check professional references of key personnel (system administrators, security officers, guards, et cetera).	Documentation of checks of professional references for key personnel.

2	• Perform background checks/screening for key personnel and external contractors, when needed and legally permitted.
	• Set up a policy and procedure for background checks.
	• Individuals screening criteria is established and reviewed for organization's position.
		• Policy and procedure for background checks/screenings. Guidance for personnel about when/how to perform background checks/screenings.
		• Screening records containing at least:
		  ○ Employment history;
		  ○ Verification of the highest education degree received;
		  ○ Residency;
		  ○ Law enforcement records.

3	• Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	• Review comments or change logs of the policy/procedures. • Documented screening requirements.

LEVEL	SECURITY MEASURES	EXAMPLES
	• The screening process is in line with the defined policies and regulations. • Individuals are rescreened based on a defined list of conditions.	• Records of rescreening process.

Mapping

ISO27001: A.7.1 Human resource security - Prior to employment

CSA CCM: CSA CCM, (HRS-02) Human Resources

BSI C5: HR-01

CCS: 5.11 System Administration and Management, 5.13 User Management and Authentication, 6.10 Employee Management

OCF: OFC, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources

NIST: PR. IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.7

2.8 SO 06 – Security knowledge and training

Description

The DSP verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training. This is achieved through for example, security awareness raising, security education, security training etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Regularly provide key personnel with relevant training and material on security issues. • Ensure that third parties are trained and aware of security issues	• Key personnel has followed security trainings and has sufficient security knowledge (interview). • Third parties have sufficient security knowledge (interview).
2	• Implement a program for training, making sure that key personnel	• Personnel have participated in awareness sessions on security topics.

LEVEL	SECURITY MEASURES	EXAMPLES
	have sufficient and up-to-date security knowledge. • The program is approved by the management. • Organize trainings and awareness sessions for personnel on security topics important for the organization.	• Documented program for training on security skills, including, objectives for different roles and how to reach it (by e.g. training, awareness raising, etc.). • Records of individual awareness activities.
3	• Contents of security training are based on assigned roles and responsibilities and specific requirements of the organization and the information system to which personnel have authorized access. • Review and update the training program periodically, taking into account changes and past incidents. • Test the security knowledge of personnel. • Contacts and communication channels with security groups and associations have been established in order to stay up to date with the latest recommended security practices, techniques, and technologies. • Provide to the organization personnel training sessions to obtain recognized security certifications.	• Updated security awareness and training program. • The last planned review has been done according with the review process. • Meeting minutes of review sessions. • List of contacts with security groups and associations. • Results of tests of the security knowledge of personnel. • Review comments or change logs for the program. • Results of individual certification process.

Mapping

ISO27001: A.7.2.2, A.6.1.1, A.7.2.2

CSA CCM: CCS CCM (HRS-08, HRS-09) Human Resources

BSI C5: HR-02, HR-03, SA-01

COBIT5: COBIT 5 APO07.03, BAI05.07, COBIT 5 APO07.02, DSS06.03, COBIT 5 APO07.03, APO10.04, APO10.05, COBIT 5 APO07.03

CCS: CCS, 5.11 System Administration and Management, 5.13 User Management and Authentication, 6.10 Employee Management

OCF: OCF, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11 Business Continuity Management & Operational Resilience, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05

NIST: PR.AT-1: All users are informed and trained

PCI-DSS: Requirement 6 - Develop and maintain secure systems and applications: 6.5, Requirement 9: Restrict physical access to cardholder data: 9.9, 9.9.3, Requirement 12: Maintain a policy that addresses information security for all personnel:12.6.1, 12.10.4, A3.1 - Implement a PCI DSS compliance program: A3.1.4

2.9 SO 07 – Personnel changes

Description

The DSP establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Following changes in personnel revoke access rights, badges, equipment, et cetera, if no longer necessary or permitted. Brief and educate new personnel on the policies and procedures in place.	• Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, et cetera • Evidence that new personnel has been briefed and educated about policies and procedures in place.
2	• Implement policy/procedures for personnel changes, taking into account timely revocation access rights, badges, equipment.	• Documentation of process for personnel changes, including, responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles.

LEVEL	SECURITY MEASURES	EXAMPLES
	• Implement policy/procedures for education and training for personnel in new roles.	• Evidence that personnel changes have been carried according to the process and that access rights have been updated timely (e.g. checklists).
3	• Periodically check that the policy/procedures are effective. • Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents. • Automated process review access permissions that are initiated by personnel changes.	• Evidence of checks of access rights etc. Up to date policy/procedures for managing personnel changes. • Review comments or change logs. • Proof of automated process.

Mapping

ISO27001: A.7.3.1

CSA CCM: CSA CCM, (HRS-04) Human Resources

BSI C5: HR-02, HR-05

CCS: 5.11 System Administration and Management, 5.13 User Management and Authentication, 6.10 Employee Management

OCF: HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources

NIST: PR. IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening

PCI-DSS: A3.2- Document and validate PCI DSS scope: A3.2.3

2.10 SO 08 – Physical and environmental security

Description

The DSP establishes and maintains policies and measures for physical and environmental security of datacenters such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Prevent unauthorized physical access to facilities and infrastructure and set up environmental controls, to protect against unauthorized access, burglary, fire, flooding, etc. • A list of personnel with authorized access to facilities containing information systems and appropriate authorization credentials (e.g., badges, identification cards) is maintained by the organization. • Visitors are authenticated before authorizing access to the facility. • Data center environmental conditions (e.g., water, power, temperature and humidity controls) shall be secured, monitored, maintained, and tested to ensure protection from unauthorized interception or damage.	• Basic implementation of physical security measures and environmental controls, such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, CCTVs, et cetera. • List of personnel with authorized access. • List of authorized visitors. • Basic implementation of environmental controls.
2	• Implement a policy for physical security measures and environmental controls. • Document procedure for emergency cases • A designated official within the organisation to review and approve the list of personnel with authorized access has been identified. • Visitors are escorted as required according to security policies and procedures. • Visitor's access records to the facility are maintained by the organisation. • The Physical access to the premises is monitored by the organisation. • Industry standard implementation of physical and environmental controls.	• Documented policy for physical security measures and environmental controls, including description of facilities and systems in scope. • Documented procedure with the specific steps to take in case of emergency. • Physical and environmental controls, like electronic control of entrance and audit trail, segmentation of spaces according to authorization levels, automated fire extinguishers with halocarbon gases, et cetera. • Records of visitors' access to the facility. • Documented description of monitoring equipment.
3	• Evaluate the effectiveness of physical and environmental controls periodically.	• Up to date policy for physical security measures and environmental controls. • Documentation about evaluation of environmental control, review comments or change logs. • Proof of different versions of physical access records.

LEVEL	SECURITY MEASURES	EXAMPLES
	• Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents. • Physical access records are kept and stored in case of an audit or investigation. • Physical access records are retained as dictated by applicable regulations or based on an organization-defined period by approved policy. • Separate facilities into different zones according to their contents.	• Documented defined period of retention. • List with different access zones.

Mapping

ISO27001: A.11

CSA CCM: CSA CCM (DCS-01, DCS-02, DCS-03, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, DCS-10, DCS-11) - Datacenter security

BSI C5: PS-01, PS-02, PS-03, PS-04, PS-05, BCM-05

CCS: 5.17 Physical Security

OCF: OCF, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09 Datacenter Security,

HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources

NIST: ID.AM-1: Physical devices and systems within the organization are inventoried, PR.AC-2: Physical access to assets is managed and, PR.AT-5: Physical and information security personnel understand roles & responsibilities, PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met, PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

PCI-DSS: Requirement 8 - Identify and authenticate access to system components: 8.6, Requirement 9 - Restrict physical access to cardholder data: all

2.11 SO 09 – Security of supporting utilities

Description

The DSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Ensure security of supplies, such as electric power, fuel or HVC.	Security of supplies is protected in a basic way, for example, backup power and/or backup fuel is available
2	• Implement a policy for security of critical supplies, such as electrical power, fuel, etc. • Implement industry standard security measures to protect supplies and supporting facilities.	• Documented policy to protect critical supplies such as electrical power, fuel, etc., describing different types of supplies, and the security measures protecting the supplies. • Evidence of industry standard measures to protect the security of supplies, such as for example, passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.
3	• Advanced security measures to protect supplies. • Review and update policy and procedures to secure supplies regularly, taking into account changes and past incidents.	Advanced implementation controls to protect security of supplies, such as active cooling, UP, hot standby power generators, sufficient fuel delivery SLA, SLAs with fuel delivery companies, redundant cooling and power backup systems.

Mapping

ISO27001: ISO/IEC/27001 A.11.2.2

BSI C5: PS-04, BCM-05

CCS: 5.17 Physical Security

OCF: BCR-01, BCR-02, BCR-03,BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11 Business Continuity Management & Operational Resilience, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09 Datacenter Security, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security

2.12 SO 10 – Access control to network and information systems

Description

The DSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES

1	• Users and systems have unique ID's and are authenticated before accessing services or systems.
	• Implement (logical) access control mechanism for network and information systems to allow only authorized use.
		• Access logs show unique identifiers for users and systems when granted or denied access.
		• Overview of authentication and access control methods for systems and users.
		• Documented methods of access control containing at least:
		  ○ Authentication type;
		  ○ Authorization schema.

2	• Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. • Based on the results of risk analysis, choose the relevant authentication mechanisms which are deemed relevant to different types of access. • Monitor access to network and information systems, have a process for approving exceptions and registering access violations. • Security functions are restricted to the least amount of users necessary to ensure the security of the information system. • Track and monitor privileged accounts by validating their creation, use of specific authentication methods and regular reviews. • Segment information access within network and information systems based on security requirements.	• Access control policy including description of roles, groups, access rights, procedures for granting and revoking access. • Different types of authentication mechanisms for different types of access, e.g. Single-Sign-On, two-factor authentication, multi-factor authentication, etc, (including remote and WiFi mechanisms) • Log of access control policy violations and exceptions, approved by the security officer. • List of authorized users who can access to security functions. • Logs from privileged accounts' usage. • Network isolation and implementation of segmented network security zones that limit the impact of a malware incident • Segregation of duties control matrix. • Access control matrix.
3	• Evaluate the effectiveness of access control policies and procedures and	• Reports of (security) tests of access control mechanisms.

LEVEL	SECURITY MEASURES	EXAMPLES
	implement cross checks on access control mechanisms. • Access control policy and access control mechanisms are reviewed and when needed revised. • Restrictions in the number of concurrent sessions are defined and implemented by the organization.	• Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection/prevention and anomaly detection systems). • Logs of intrusion detection[10]/prevention and anomaly detection systems. • Updates of access control policy, review comments or change logs. • Real-time logging and recording of unsuccessful login attempts; • Real-time alerting when the number of defined consecutive invalid access attempts is exceeded.

Mapping

ISO27001: ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1, ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1

CSA CCM: CCA CCM (EKM-01, EKM-02, EKM-03, EKM-04) Encryption & key management

BSI C5: IDM-01, IDM-02, IDM-03, IDM-04, IDM-05, IDM-06, IDM-07, IDM-08, IDM-09, IDM-10, IDM-11, IDM-12, KOS-01, KOS-02, KOS-03, KOS-04, KOS-05, KOS-06, KOS-07, KOS-08
COBIT 5: COBIT 5 DSS05.04, DSS06.03, COBIT 5 DSS01.04, DSS05.05, COBIT 5 APO13.01, DSS01.04, DSS05.03

CCS: CCS, 5.3 Client Separation, 5.4 Security Architecture, 5.6 Network Segmentation, 5.7 Network Architecture, 5.11 System Administration and Management, 5.13 User Management and Authentication, 6.5 Data Protection

OCF: OCF, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, EKM-01, EKM-02, EKM-03, EKM-04 Encryption & Key Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11,IAM-12,IAM-13 Identity & Access Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability

NIST: PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

PCI-DSS: Requirement 1: Install and maintain a firewall configuration to protect cardholder data: all Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: all

[10] Of either known or unknown attacks or both.

2.13 SO 11 – Integrity of network components and information systems

Description

The DSP establishes, protects, and maintains the integrity of its own network, platforms and services by taking steps to prevent successful security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Make sure software of network and information systems is not tampered with or altered, for instance by using input controls. • Protect security critical data (like passwords, shared secrets, private keys, etc.) from being disclosed or tampered with. • Take measures against malicious software on (internal) network and information systems.	• Software and data in network and information systems is protected using prevention, input controls, firewalls, encryption and signing. • Security critical data is protected using protection mechanisms like separate storage, encryption, hashing, etc. • Malware detection systems are present, and up to date. • Records of recent updates of malware protection mechanisms. • Records of periodical scans.

2	• Implement industry standard security measures, providing defense-in-depth and protection against tampering and altering of systems.
	• The malware protection mechanisms are centrally managed.
	• There are mechanisms which prevent users from circumventing malware protection capabilities.
	• Spam protection mechanisms are employed at system entry points such as workstations, servers, or mobile computing devices on the network.
		• Documentation about how the protection of software and data in network and information system is implemented.
		• Documented alternative countermeasures such as:
		  ○ Securing of all physical and logical data interfaces;
		  ○ Network isolation and implementation of segmented network security zones that limit the impact of a malware incident;
		  ○ Comprehensive system hardening measures to minimize the risk of malware incidents.
		• Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection/prevention and anomaly detection systems).
		• Logs of intrusion detection/prevention and anomaly detection systems.
		• Documented description of centrally management tools.
		• Documented spam protection mechanism.
		• Use of whitelisting solutions, which restrict the execution of non-approved software and code.
		• Interactive access to critical systems is performed using hardened hosts which have built in controls to inhibit phishing attacks, lateral movement, and persistent compromise.

3	• Sophisticated controls to protect integrity of systems. • Evaluate and review the effectiveness of measures to protect integrity of systems.	• Sophisticated controls to protect integrity of systems, such as code signing, tripwire, et cetera. • Documentation of process for checking logs of anomaly and intrusion detection/prevention systems.

Mapping

ISO27001: A.13.1

BSI C5: RB-05, RB-17, RB-18, RB-23, IDM-08, IDM-11, KOS-02, KOS-03, KOS-05, BEI-01

CCS: 5.4 Security Architecture, 5.5 Encryption, 5.6 Network Segmentation, 5.7 Network Architecture, 6.5 Data Protection

OCF: CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, EKM-01, EKM-02, EKM-03, EKM-04 Encryption & Key Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11,IAM-12,IAM-13 Identity & Access Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, MOS-01,MOS-02,MOS-03,MOS-04,MOS-05,MOS-06,MOS-07,MOS-08,MOS-09,MOS-10,MOS-11,MOS-12,MOS-13 to MOS-20 Mobile Security, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability, TVM-01, TVM-02, TVM-03 Threat and Vulnerability Management

NIST: PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate, PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met

PCI-DSS: Requirement 4: Encrypt transmission of cardholder data across open, public networks

2.14 SO 12 – Operating procedures

Description

The DSP establishes and maintains procedures for the operation of key network and information systems by personnel. (i.e. operating procedures, user manual, administration procedures for critical systems etc.)

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Set up operational procedures and assign responsibilities for operation of critical systems.	Documentation of operational procedures and responsibilities for key network and information systems.
2	Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures.	Documented policy for operation of critical systems, including an overview of network and information systems in scope.

LEVEL	SECURITY MEASURES	EXAMPLES
3	Review and update the policy/procedures for operation of critical systems, taking into account incidents and/or changes.	Updated policy/procedures for critical systems, review comments and/or change logs.

Mapping

ISO27001: ISO/IEC 27001:2013 A12.1.1, A.12.5.1, A.13.2.1, A.14.2.2

CCS: 4.1 Service Desk, 4.2 Application Management, 4.3 Technical Management, 4.4 Operations Management

BSI C5: SA-01, AM-03, AM-07, PS-05, RB-06, RB-10, RB-11, RB-17, RB-19, IDM-01, KRY-01, KOS-07, PI-03, BEI-01, BEI-03, SIM-01, BCM-02, MDM-01

OCF: BCR-01, BCR-02, BCR-03,BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11 Business Continuity Management & Operational Resilience, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09 Datacenter Security, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security

2.15 SO 13 – Change management

Description

The DSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Follow predefined procedures when making changes to critical systems, according to licensing agreements • Inform the customer of significant changes to critical systems which affect the offered services.	• Documentation of change management procedures for critical systems. • Documentation of a customer update on significant changes
2	• Implement and test policy/procedures for change management, to make sure that changes of critical	• Documentation of change management policy/procedures including, systems subject to the policy, objectives, roll back procedures, etc.

LEVEL	SECURITY MEASURES	EXAMPLES
	systems are always done following a predefined way. • Document change management procedures, and record for each change the steps of the followed procedure.	• For each change, a report is available describing the steps and the result of the change
3	Review and update change management procedures regularly, taking into account changes and past incidents.	Up to date change management procedures, review comments and/or change logs.

Mapping

ISO27001: ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4

CSA CCM: CSA CCM (CCC-01, CCC-02, CC03, CC04, CC05, CC06) Change control & configuration management

BSI C5: BEI-03, BEI-04, BEI-05, BEI-06, BEI-07, BEI-08, BEI-09, BEI-10, BEI-11, BEI-12, DLL-02, BCM-02, BCM-04

COBIT 5: COBIT 5 BAI06.01, BAI01.06

CCS: 4.2 Application Management, 4.4 Operations Management, 7.5 Change Management

OCF: DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09 Datacenter Security, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security

NIST: PR. IP-3: Configuration change control processes are in place

PCI-DSS: Requirement 6: Develop and maintain secure systems and applications: 6.4.6, Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.1.1.1, A3.2- Document and validate PCI DSS scope: A3.2.2.1, A3.4.1

2.16 SO 14 – Asset management

Description

The DSP establishes and maintains asset management procedures and configuration controls for key network and information systems.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES

1	• A secure baseline configuration of components and information systems is developed, documented and maintained.
	• Manage critical assets e.g. software, hardware, information and configurations of critical systems.
		• Documented secure baseline configuration containing at least:
		  ○ Essential capabilities of operation;
		  ○ Restricted use of functions;
		  ○ Security by default;
		  ○ Ports, protocols and/or services allowed.
		• List of critical assets and critical systems.

2	Implement policy/procedures for asset management and configuration control.	• Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, the objectives of asset management • 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.
3	• Review and update the asset management policy regularly, based on changes and past incidents. • Review regularly the list with configurations and the list with critical assets based, based on changes and past incidents. • A secure baseline configuration for development and test environments is managed separately from the operational baseline configuration.	• Up to date asset management policy/procedures, review comments and/or change logs. • Documented results of the review activities. • Documented and approved exceptions to the configuration baseline containing the alternative controls in place to ensure the confidentiality, availability and integrity of the information system. • Documented secure baseline configuration for development and test environments.

Mapping

ISO27001: ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, ISO/IEC 27001:2013 A.13.2.1, ISO/IEC 27001:2013 A.8.2.1, ISO/IEC 27001:2013 A.6.1.1

CSA CCM: (DSI-01) Datacenter security - Asset management, (HRS-01) Human resources- Asset returns

BSI C5: AM-01, AM-02, AM-03, AM-04, AM-05, AM-06, AM-07, AM-08
COBIT 5: BAI09.01, BAI09.02, COBIT 5 BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO01.02, DSS06.03

CCS: 4.2 Application Management, 5.1 Principles of Cloud Architecture, 5.16 Data Management, 6.1 Location of Data and Data Centers, 7.6 Service Asset and Configuration Management

OCF: DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09 Datacenter Security, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security

NIST: PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.1, 12.2

2.17 SO 15 – Security incident detection & Response

Description

The DSP establishes and maintains procedures for detecting and responding to security incidents appropriately. These should consider detection, response, mitigation, recovery and remediation from a security incident. Lessons learned should also be adopted by the service provider.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Set up processes or systems for incident detection and response. • Make sure personnel is available and prepared to manage and handle incidents.	• Past incidents were detected and timely forwarded to the appropriate people, including customers. • Personnel is aware of how to deal with incidents and when to escalate. • Inventory of major incidents and per incident, impact, cause, actions taken, and lessons learnt.
2	• Implement industry standard systems and procedures for incident detection and response.	• 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, et cetera.

LEVEL	SECURITY MEASURES	EXAMPLES

	• Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	• Policy/procedures for incident detection and response, including, types of incidents that could occur, objectives, roles and responsibilities, detailed description, per incident type, how to manage the incident, when to escalate to senior management (CISO e.g.), et cetera.
		• Management commitment with the incident response program.
		• Records of individual training activities.
		• Description of the incident handling capability containing at least the following procedures:
		  ○ Preparation;
		  ○ Detection;
		  ○ Analysis;
		  ○ Containment;
		  ○ Mitigation;
		  ○ Recovery.

3	• Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate and reduce time to react to any future occurrence of this type of incident or data breach. • Review systems and processes for incident detection and response regularly and update them taking into account changes and past incidents. • Regular cyber exercises and related results to test the incident response effectiveness are scheduled and documented.	• Individual reports of the handling of major incidents. • Up to date documentation of incident detection and response systems and processes. • Documentation of review of the incident detection and response processes, maximum response times, review comments, and/or change logs. • Records of cyber exercises.

Mapping

ISO27001: ISO/IEC 27001:2013 A.16.1.5

CSA CCM: (SEF-03, SEF-04, SEF-05) Security incident management (reporting & response metrics)

BSI C5: SIM-01, SIM-02, SIM-03, SIM-04, SIM-05, SIM-06, SIM-07, RB-10, RB-11, RB-14, RB19, RB-20, DLL-01, DLL-02

COBIT 5: BAI01.10

CCS: 4.1 Service Desk, 5.18 Response to Security Incidents, 6.12 Security Management, 7.1 Resolution Processes

OCF: CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05 Security Incident Management, E-Discovery & Cloud Forensics

NIST: DE.AE-5: Incident alert thresholds are established, RS.AN-2: The impact of the incident is understood

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.10, 12.10.1. 12.10.2

2.18 SO 16 – Security incident reporting

Description

The DSP establishes and maintains appropriate procedures for reporting and communicating about security incidents.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES

1	Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.	• List of authorities contacts containing at least:
		  ○ National and international agencies together with structures for co-operation for the protection of critical infrastructures;
		  ○ National and international CERT organizations;
		  ○ Disaster control organizations and disaster-relief teams;
		  ○ Documented communication channels.
		• Evidence of past communications and incident reporting.

2	Implement policy and procedures for communicating and reporting about 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

LEVEL	SECURITY MEASURES	EXAMPLES
		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. • Templates for incident reporting and communication.
3	• Evaluate past communications and reporting about incidents. • Review and update the reporting and communication plans, based on changes or past incidents.	• List of incident reports and past communications about incidents • Up to date incident response and communication policy, review comments, and/or change logs.

Mapping

ISO27001: ISO/IEC 27001:2013 A.16.1.5

CSA CCM: CSA CMM (SEF-01, SEF-02, SEF-04,) Security incident management (contact/authority maintenance, management & legal preparations)

BSI C5: SIM-04, SIM-06, OIS-03, DLL-01, DLL-02

COBIT 5: EDM03.02, MEA03.02

CCS: 4.1 Service Desk, 5.18 Response to Security Incidents, 6.12 Security Management, 7.1 Resolution Processes

OCF: CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12,IVS-13 Infrastructure & Virtualization Security, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05 Security Incident Management, E-Discovery & Cloud Forensics

NIST: PR. IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.10.2, 12.10.4, 12.10.5, 12.10.6

2.19 SO 17 – Business continuity

Description

The DSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Implement a service continuity strategy for the communications networks and/or services provided.	• Documented service continuity strategy, including recovery time objectives for key services and processes. • Management commitment with the continuity strategy.
2	• Implement contingency plans for critical systems. • Monitor activation and execution of contingency plans, registering successful and failed recovery times.	• Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives. • Decision process for activating contingency plans. • Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time.
3	• Review and revise service continuity strategy periodically. • Review and revise contingency plans, based on past incidents and changes. • The continuity of operations plan is tested and updated on a regular basis. • Personnel involved in the continuity operations plan are trained in their roles and responsibilities with respect to the information system and receive refresher training on an organization-defined frequency.	• Up to date continuity strategy and contingency plans, review comments, and/or change logs. • Documented results of the continuity of operations test activities. • Records of individual training activities.

Mapping

ISO27001: ISO/IEC/27001:2013 A.17.1

CSA CCM: (BCR-01, BCR-02, BCR-03, BCR-04-BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11) Business continuity management & operational resilience retention policy

BSI C5: BCM-01, BCM-02, BCM-03, BCM-04, BCM-05

CCS: 5.12 Backup, 7.2 IT Service Continuity Management

OCF: BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11 Business Continuity Management & Operational Resilience, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management

NIST: PR. IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.10.1

2.20 SO 18 – Disaster recovery capabilities

Description

The DSP establishes and maintains an appropriate disaster recovery capability for restoring the offered services in case of natural and/or major disasters.

Security measures within sophistication levels[11]

LEVEL	SECURITY MEASURES	EXAMPLES
1	Prepare for recovery and restoration of services following disasters.	Measures are in place for dealing with disasters, such as failover sites in other regions, backups[12] of critical data to remote locations, et cetera.
2	• Implement policy/procedures for deploying disaster recovery capabilities. • Implement industry standard disaster recovery capabilities or be assured they are available from third parties (such as national emergency networks).	• 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 parties). • Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, et cetera.

[11] At the basic sophistication level this objective could be merged with SO 17: 'Business continuity' into one.
[12] Backup solutions should be disconnected from live systems because some forms of ransomware might encrypt backups attached to the system.

LEVEL	SECURITY MEASURES	EXAMPLES
3	• Advanced implementation controls for disaster recovery capabilities to mitigate natural and/major disasters. • Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	• Advanced implementation controls for disaster recovery capabilities, such as full redundancy and failover mechanisms to handle natural and/or major disasters. • Data centre infrastructure/design is designed for availability, auto failover, and resiliency to maintain service to customers. • Updated documentation of disaster recovery capabilities in place, review comments and/or change logs.

Mapping

ISO27001: ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2

CSA CCM: (BCR-09, BCR-11) Business continuity management & operational resilience retention policy

BSI C5: BCM-04, BCM-05

COBIT 5: DSS04.03

CCS: 5.1 Principles of Cloud Architecture, 5.12 Backup, 7.2 IT Service Continuity Management

OCF: BCR-01, BCR-02, BCR-03,BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11 Business Continuity Management & Operational Resilience, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management

NIST: PR. IP-10: Response and recovery plans are tested

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.10.1

2.21 SO 19 – Monitoring and logging

Description

The DSP establishes and maintains procedures and systems for monitoring and logging of the offered services (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.).

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Implement monitoring and logging of critical systems.	Logs and monitoring reports of critical network and information systems.

LEVEL	SECURITY MEASURES	EXAMPLES

2	• Implement policy for logging and monitoring of critical systems.
	• Set up tools for monitoring critical systems.
	• Set up tools to collect and store logs critical systems.
		• List of auditable events.
		• Audit records containing at least:
		  ○ Date and time of the event;
		  ○ Component of the information system where the event concurred;
		  ○ Type of event;
		  ○ User/subject identity;
		  ○ Outcome of the event.
		• Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs.
		• Tools for monitoring systems and collecting logs.
		• List of monitoring data and log files, in line with the policy.

3	• Set up tools for automated collection and analysis of monitoring data and logs. • Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	• Tools to facilitate structural recording and analysis of monitoring and logs. • Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs.

Mapping

ISO27001: ISO/IEC 27001:2013 A.12.4

CSA CCM: CSA CCM (IVS-01)- Infrastructure & Virtualization Security (Audit Logging / Intrusion Detection)

BSI C5: RB-02, RB-07, RB-10, RB-11, RB-12, RB-13, RB-14, RB-15, RB-16, KOS-02, DLL-02

CCS: 5.11 System Administration and Management

OCF: OCF, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12, IVS-13 Infrastructure & Virtualization Security

NIST: DE.CM: Security continuous monitoring

PCI-DSS: A1: Additional PCI DSS Requirements for Shared Hosting Providers: A1.3

2.22 SO 20 – System tests

Description

The DSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Test networks and information systems before using them or connecting them to existing systems. • The installation or de-installation of patches is done in an ad hoc manner.	• Test reports of the network and information systems, including tests after big changes or the introduction of new systems. • Checks for latest patches

2	• Implement policy/procedures for testing network and information systems.
	• Implement tools for automated testing.
	• The installation or de-installation of patches is done periodically in an organized manner.
		• Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates.
		• Documented testing activities containing at least:
		  ○ Objectives, roles, and responsibilities;
		  ○ Scope of the plan;
		  ○ Detailed results of the execution of the plan;
		  ○ Frequency of the test.
		• Approved documented actions applying patches.

3	• Review and update the policy/procedures for testing, taking into account changes and past incidents. • The installation or de-installation of patches is reviewed to ensure the adequately implementation of the defined actions. • Exceptions to defined actions and approved mitigating actions are identified and documented.	• List of test reports. • Updated policy/procedures for testing networks and information systems, review comments, and/or change log.

Mapping

ISO27001: ISO/IEC 27001:2013 A.14.2

BSI C5: RB-18, RB-21, BEI-01, BSI-02, BEI-03, BEI-07, BEI-09

CCS: 4.3 Technical Management, 6.2 Compliance Management, 6.4 Audit Management, 6.12 Security Management

OCF: OCF, AIS-01, AIS-02, AIS-03, AIS-04 Application & Interface Security, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, MOS-01,MOS-02,MOS-03,MOS-04,MOS-05,MOS-06,MOS-07,MOS-08,MOS-09,MOS-10,MOS-11,MOS-12,MOS-13 to MOS-20 Mobile Security, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability, TVM-01, TVM-02, TVM-03 Threat and Vulnerability Management

NIST: PR. IP-10: Response and recovery plans are tested

PCI-DSS: A3.2- Document and validate PCI DSS scope: A3.2.4, A3.2.5.1

2.23 SO 21 – Security assessments

Description

The DSP establishes and maintains appropriate procedures for performing security assessments of critical assets.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes. • Vulnerabilities are monitored and assessed.	• Reports from past security scans and security tests. • Documented vulnerability scans reports.
2	• Implement policy/procedures for security assessments and security testing. • A single point of contact and communication channels for information security related issues with manufacturers or vendors have been identified.	• Documented policy/procedures for security assessments and security testing, including, which assets, in 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. • List of manufactures single point of contact.

LEVEL	SECURITY MEASURES	EXAMPLES
3	• Evaluate the effectiveness of policy/procedures for security assessments and security testing. • Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents. • Information obtained from the vulnerability scanning process is shared with designated personnel throughout the organization and authorities to help eliminate similar vulnerabilities in other information systems.	• List of reports about security assessments and security tests. • Reports of follow up actions on assessments and test results. • Up to date policy/procedures for security assessments and security testing, review comments, and/or change log. • Records of vulnerabilities information sharing.

Mapping

ISO27001: ISO/IEC 27001:2013 A.12.6.1, A.18.2.2

CSA CCM: (AAC-02) Audit assurance & compliance independent audits

BSI C5: COM-02, COM-03, RB-17, RB-18, RB-19, RB-21

CCS: 6.2 Compliance Management, 6.4 Audit Management, 6.12 Security Management, 6.13 Embedding External Services

OCF: OCF, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, MOS-01,MOS-02,MOS-03,MOS-04,MOS-05,MOS-06,MOS-07,MOS-08,MOS-09,MOS-10,MOS-11,MOS-12,MOS-13 to MOS-20 Mobile Security, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability

PCI-DSS: Requirement 6: Develop and maintain secure systems and applications: 6.6

2.24 SO 22 – Compliance

Description

The DSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Monitor compliance to standards and legal requirements.	Reports describing the result of compliance monitoring.
2	Implement policy/procedures for compliance monitoring and auditing.	• Documented policy/procedures for monitoring compliance and auditing, including what (assets, processes, infrastructure), frequency, guidelines who should carry out audits (in- or external), relevant security policies that are subject to compliance monitoring and auditing, the objectives and high level approach of compliance monitoring and auditing, templates for audit reports. • Detailed monitoring and audit plans, including long term high level objectives and planning.
3	• Evaluate the policy/procedures for compliance and auditing. • Perform deviation root cause analysis. • Build remediation plans for critical assets. • Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents.	• List of all compliance and audit reports ○ Root cause analysis to the compliance and audit reports. • Remediation plans for critical assets. • Updated policy/procedures for compliance and auditing, review comments, and/or change logs.

Mapping

ISO27001: ISO/IEC/27001:2013 A.18

CSA CCM: CSA CCM (AAC-01, AAC-02, AAC-03) Audit assurance & compliance

BSI C5: COM-01, COM-02, COM-03

COBIT 5: 5.15 Configuration Management, 6.2 Compliance Management, 6.4 Audit Management, 6.12 Security Management, 6.13 Embedding External Services

OCF: OCF, AAC-01, AAC-02, AAC-03 Audit Assurance & Compliance, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, EKM-01, EKM-02, EKM-03, EKM-04 Encryption & Key Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11 Human Resources, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11,IAM-12,IAM-13 Identity & Access Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, MOS-01,MOS-02,MOS-03,MOS-04,MOS-05,MOS-06,MOS-07,MOS-08,MOS-09,MOS-10,MOS-11,MOS-12,MOS-13 to MOS-20 Mobile Security, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05 Security Incident Management, E-Discovery & Cloud Forensics, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and accountability

2.25 SO 23 – Security of data at rest

Description

The DSP establishes and maintains appropriate mechanisms for the protection of the data at rest[13].

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Identify the most critical data taking into account relevant business needs and legal obligations (e.g. with regard to the processing of personal data). • Retain the critical data for a certain period depending on the type of data and its criticality • Implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas and in transit when moving within and between company data locations. • Implement cryptographic mechanisms such as digital signatures and hashes to detect unauthorized changes to critical data at rest. • Implement mechanisms for the secure disposal of the data after their lawful use.	• The access control, sharing, copying, transmittal and distribution of confidential and restricted data are defined • Safeguards to protect the secrecy of secret (private) key(s) are in place • Limited or ad hoc processes exist to protect electronic media • Evidence from regular reviews of devices/storage media to examine that data is removed or securely overwritten prior to disposal.
2	• Classify all data according to a classification scheme which takes into account data's value, legal requirements, sensitivity, and criticality to the organization. • Use of removable media is prohibited unless strictly required. • Ensure the confidentiality and integrity of data at rest according to the classification scheme. • Establish a policy around confidentiality and integrity of data at rest and make all personnel to whom it is relevant, are aware of the policy and procedure and what it implies for their work. • Set detailed cryptographic key establishment and management policies and procedures for data at rest (only if cryptography has been implemented).	• Data retention policy exists and is complete • Formal standard to govern protection of electronic transportable media is in place. Encryption enforced on electronic media identified with confidential information. • Evidence for the existence of mechanisms which support in ensuring confidentiality and integrity of the data at rest such as cryptographic mechanisms, file share scanning, secure offline storage, removal of sensitive data from storage media etc. according to the classification scheme. • Evidence of the existence of a mechanism (either manual or automated) for the establishment and management of cryptographic keys (only if cryptography has been implemented).

[13] The term 'data at rest' is extensively used to collectively describe different types of data formats such as databases, office data and data stored in various types of storage media.

LEVEL	SECURITY MEASURES	EXAMPLES
	• A set of best practice procedures are in place for the secure disposal of physical assets.	• Obtain evidence of written authorization to dispose of equipment from department Head. A disposal form should be completed.
3	• Classify all assets according to the classification scheme. • Implement information labelling and handling procedures in accordance with the classification scheme • The data retention policy considers the value of data over time and the data retention laws the organization may be subject to. • Strong controls are in place surrounding connection of media devices. • Use automated key management mechanisms. • Review of confidentiality and integrity of data at rest policy. • Disposal of assets at the most opportune time in line with company objectives, strategy and the data retention policy, using the most appropriate methods.	• Labelling of information of information is reviewed on a regular basis • The data retention policy is supported by a comprehensive data retention schedule, which contains the retention period for each type of data used by the organization • Reports of the data retention policy and configuration which ensure that they are in line with requirements and good practices • Technology infrastructure automatically encrypts and protects electronic transportable media in the environment. • Portable media standards are reviewed at least annually and on an ad hoc basis for any new technology or threats. • Evidence that the public-key encryption and secret key of user and cipher-text are based on the subject's attributes. • Documentation of review process, taking into account changes and past incidents. Review the policy on a regular basis • Personnel are aware of the confidentiality and integrity of the data at rest policy and procedures and what it implies for their work (interview). Review comments or change logs for the policy and/or procedure. • Evidence of secure key generation, use, storage and destruction of data. • Rationale for disposal of assets and the methods used is provided. Review of physical asset inventory. All devices leaving the controlled environment must be purged of data using disk wiping utilities or degassing methods (reformatting is not enough)

Mapping

ISO27001: ISO/IEC 27001:2013 A.8.2.3, ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3, ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, ISO/IEC 27001:2013 A.12.1.4

CSA CCM: (DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07) Data security

BSI C5: AM-05, SIM-02, RB-10, COM-01, KRY-01, KRY-02, KRY-03, KRY-04, PI-05, RB-11, RB-13, AM-04, AM-07, RB-23, KOS-05, BEI-03, HR-02, HR-03

COBIT 5: APO01.06, BAI02.01, BAI06.01, DSS06.06

CCS: 5.1 Principles of Cloud Architecture, 5.2 Development Processes, 5.3 Client Separation, 5.5 Encryption, 5.7 Network Architecture, 5.9 Virtualization, 5.13 User Management and Authentication, 5.16 Data Management, 6.5 Data Protection

OCF: OCF, AIS-01, AIS-02, AIS-03, AIS-04 Application & Interface Security, AAC-01, AAC-02, AAC-03 Audit Assurance & Compliance, BCR-01, BCR-02, BCR-03,BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11 Business Continuity Management & Operational Resilience, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09 Datacenter Security, EKM-01, EKM-02, EKM-03, EKM-04 Encryption & Key Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11,IAM-12,IAM-13 Identity & Access Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability

NIST: Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

PCI-DSS: Requirement 12 - Maintain a policy that addresses information security for all personnel: 12.6

2.26 SO 24 –Interface security

Description

The DSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data. [14]

[14] Customer interface is considered a powerful tool offered by the DSPs to the customers as a means to enhance customer's control on his own data in the cloud.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Set a high level security policy for keeping the cloud and online market interfaces secure • Make key personnel aware of the security policy. • Enable secure channels for data transmission (e.g. TLS2.0) • Use unique identifiers to identify users	• Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. • Key personnel are aware of the security policy and its objectives (interview). • At least one secure channel is enabled. • All customers are assigned to a unique identifier.
2	• Set detailed security policies for data security to include protection of customer administration interfaces (TLS2.0, 2-Factor authentication) etc. • Make all personnel aware of the security policy and what it implies for their work. • Review the security policy following incidents. • Implement 2-Factor authentication	• Documented security policies, approved by management, including applicable law and regulations, accessible to personnel. • Personnel are aware of the security policy and what it implies for their work (interview). • Review comments or change logs for the policy.
3	• Review the security policy periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	• Security policies are up to date and approved by senior management. • Logs of policy exceptions, approved by the relevant roles. • Documentation of review process, taking into account changes and past incidents.

Mapping

CSA CCM: (AIS-01, AIS-02, AIS-03, AIS -04) Application & Interface Security

BSI C5: OIS-02, SA-01, PI-01, HR-02, HR-03, KRY-01, KRY-02, SIM-07, SIM-01, SIM-03, SIM-04, SIM-05, SIM-06 IDM-08

CCS: 5.1 Principles of Cloud Architecture, 5.2 Development Processes, 5.4 Security Architecture

OCF: OCF, AIS-01, AIS-02, AIS-03, AIS-04 Application & Interface Security, EKM-01, EKM-02, EKM-03, EKM-04 Encryption & Key Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11,IAM-12,IAM-13 Identity & Access Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability,

PCI-DSS: Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: 2.3

2.27 SO 25 –Software security

Description

The DSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security[15].

Security measures within sophistication levels[16]

LEVEL	SECURITY MEASURES	EXAMPLES
1	Establish guidelines for maintaining software security	• Documented guidelines, to ensure that software security is maintained. • Key personnel are aware of the guidelines and its objectives (interview).
2	• Implement a defined set of security measures to secure development environments, including measures for protecting test data. • Depending on the type of requirement include software testing methods (e.g. black-box, ad-hoc testing).	• Evidence of the test results to secure development environments, including measures for protecting test data are maintained. • Evidence of the software testing methods chosen for a particular test scenario and explanation of this.

[15] In case that software development is outsourced the DSP should take provisions to include Software Lifecycle Agreements (SLA) as an essential part of the procurement process.
[16] Although patching has been already described under SO 13: 'Change Management', one can include it under this objective as well.

LEVEL	SECURITY MEASURES	EXAMPLES
	• Keep separated environments for development purposes, testing purposes and production.	• Evidence of separated environments for development, testing and production.
3	• Security by design is tested at various stages of the SDLC prior to Go-live utilizing independent tools and a self-service testing platform throughout SDLC. • Results of application assessments are used to regularly enhance developer training and the SDLC process. •	• Test results of each phase of the SDLC are maintained and are up to date. Test results are maintained and approved by senior management • Documented evidence of the review process of the patch development process, security training for software developments and secure by design software configurations • Evidence that a software testing method is chosen at each stage of the software development lifecycle

Mapping

CSA CCM: (AIS -04) -Application & Interface Security/Data Security Integrity

BSI C5: BEI-01, BEI-02

CCS: 5.1 Principles of Cloud Architecture, 5.2 Development Processes, 5.9 Virtualization, 5.14 Patch Management

OCF: OCF, AIS-01, AIS-02, AIS-03, AIS-04 Application & Interface Security, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05 Change Control & Configuration Management, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07 Data Security & Information Lifecycle Management, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11 Governance and Risk Management, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11,IVS-12,IVS-13 Infrastructure & Virtualization Security, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability, MOS-01,MOS-02,MOS-03,MOS-04,MOS-05,MOS-06,MOS-07,MOS-08,MOS-09,MOS-10,MOS-11,MOS-12,MOS-13 to MOS-20 Mobile Security, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09 Supply Chain Management, Transparency and Accountability, TVM-01, TVM-02, TVM-03 Threat and Vulnerability Management

NIST: ID.AM-2: Software platforms and applications within the organization are inventoried, ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value, PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity, DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed

PCI-DSS: Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters: 2.4

2.28 SO 26 – Interoperability and portability

Description

Online market place and cloud providers use standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	Implement processes and procedures which allow customers to interact with services and/or if needed to migrate to other providers offering similar services, in an easy and basic way	• Use of HTML/XML which allow users to integrate different services and to (more easily) migrate from one provider to another • Use of OVF standard format for virtual machines
2	Implement industry standard security measures, which promote interoperability and portability, including fall-back procedures (for example in the case of cloud computing services).	• Use of SAML/XACML that acts as an interface to manage the provision of identification and user authentication between user and provider • Documentation about how the protection and integrity of infrastructure & virtualization security is maintained. • Information on the fallback procedures is explicitly described.
3	• Set up state of the art controls to facilitate interoperability & portability. • Evaluate and review the effectiveness of interoperability & portability measures.	• State of the art controls exist and are a crucial aspect to mitigate security related risks for customers • Where applicable, tools for detection of anomalous usage or risks associated is used, which allows the option for customer to plan in advance the interoperability & portability measures.

Mapping

CSA CCM: (IPY-01, IPY-02, IPY-03, IPY-04, IPY-05) - Interoperability & Portability

BSI C5: PI-01, PI-02, PI-03, PI-04, PI-05

CCS: 5.8 Network Monitoring, 5.10 System Monitoring

OCF: IPY-01, IPY-02, IPY-03, IPY-04, IPY-05 Interoperability & Portability

2.29 SO 27 – Customer Monitoring and log access

Description

The cloud provider grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed.

Security measures within sophistication levels

LEVEL	SECURITY MEASURES	EXAMPLES
1	• Separate the logging information between the different customers. • Implement monitoring and logging of customer data.	• Logs and monitoring reports available to customer concerning his data.
2	• Implement policy for logging and monitoring of customer data depending on the type of service. • Set up tools for customer to monitor this data • Set up tools to collect and store logs of customer data.	• 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. • Tools for monitoring systems and collecting customer data logs. • List of monitoring customer data and log files, in line with the policy.
3	• Set up tools for automated collection and analysis of monitoring data and logs. • Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	• Tools to facilitate structural recording and analysis of monitoring and logs of customer data. • Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs.

Mapping

ISO27001: ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3 & A.12.4.4

CSA CCM: (IVS-01)- Infrastructure & Virtualization Security, (Audit Logging / Intrusion Detection)

BSI C5: RB-13H, RB-14, RB14H, RB-10, RB-11, RB-12, RB-13, RB-15, RB-16H, RB-23

COBIT 5: APO11.04

CCS: 5.8 Network Monitoring, 5.10 System Monitoring

OCF: IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12, IVS-13 Infrastructure & Virtualization Security

NIST: PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy, PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools

3. Summary

To summarise, the level of sophistication to which security measures are implemented from one organization to another can vary for a multitude of reasons. For instance, this may depend on the industry sector, the size of the company or the time and effort that the management can afford to invest in implementing security measures. From the received feedback for this study, stakeholders should consider the different roles that the DSP's play in the online environment, and in particular how their level of criticality differs (i.e. lack of availability for a search engine may not pose a significant risk, whereas for a different DSP, this may be more critical). As a result, some security objectives may be prioritized over others and thus the sophistication levels may also differ.

There are high level security objectives, which are interchangeable among all three DSP categories, while a few belong to specific DSP categories. In the following table, the common security objectives for all DSPs are marked with a check mark. If a SO doesn't belong to a specific DSP category, it is indicated with an xmark.

SECURITY OBJECTIVES	CLOUD PROVIDERS	ONLINE MARKET PLACES	ONLINE SEARCH ENGINES
SO 01 - Information security policy	✓	✓	✓
SO 02 – Risk Management	✓	✓	✓
SO 03 – Security Roles	✓	✓	✓
SO 04 – Third party management	✓	✓	✓
SO 05 – Background checks	✓	✓	✓
SO 06 – Security knowledge and training	✓	✓	✓
SO 07 – Personnel changes	✓	✓	✓
SO 08 – Physical and environmental security	✓	✓	✓
SO 09 – Security of supporting utilities	✓	✓	✓
SO 10 – Access control to network and information systems	✓	✓	✓
SO 11 – Integrity of network components and information systems	✓	✓	✓
SO 12 – Operating procedures	✓	✓	✓
SO 13 – Change management	✓	✓	✓
SO 14 – Asset management	✓	✓	✓
SO 15 – Security incident detection & Response	✓	✓	✓
SO 16 – Security incident reporting	✓	✓	✓
SO 17 – Business continuity	✓	✓	✓
SO 18 – Disaster recovery capabilities	✓	✓	✓
SO 19 – Monitoring and logging	✓	✓	✓
SO 20 – System tests	✓	✓	✓

SO 21 – Security assessments	✓	✓	✓
SO 22 – Compliance	✓	✓	✓
SO 23 –Security of data at rest	✓	✓	✓
SO 24 –Interface security	✓	✓	✓
SO 25 –Software security	✓	✓	✓
SO 26 – Interoperability and portability	✓	✓	×
SO 27 – Customer Monitoring and log access	✓	×	×

Finally, we present a summary table below with a mapping of the SOs to the different schemes. If a security objective is covered in one of the schemes below it is marked with a dot. If not, it stays blank.

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO1 Information Security Policy	●	●	●		●	●	●	●	
SO2 Risk management	●	●	●		●	●	●	●	
SO3 Security roles	●	●	●		●	●	●	●	
SO 04 Security in supplier relationships	●	●	●		●	●	●	●	
SO 05 Background checks	●	●	●		●	●	●	●	
SO 06 Security knowledge and training	●	●	●	●	●	●	●	●	
SO 07 Personnel changes	●	●	●		●	●	●	●	
SO 08 Physical and environmental security	●	●	●		●	●	●	●	
SO 09 Security of supporting utilities	●		●		●	●			
SO 10 Access control to network and information systems	●	●	●	●	●	●	●	●	●
SO 11 Integrity of network and information systems	●		●		●	●	●	●	●
SO 12 Operating procedures	●				●	●			●
SO 13 Change management	●	●	●	●	●	●	●	●	●
SO 14 Asset management	●	●	●	●	●	●	●	●	●
SO 15 Security incident detection & response	●	●	●	●	●	●	●	●	
SO 16 Security incident reporting	●	●	●	●	●	●	●	●	
SO 17 Business continuity	●	●	●		●	●	●	●	

[17] Including CES+

SECURITY OBJECTIVES	ISO27001	CSA CCM	BSI C5	COBIT 5	CCS	OCF	NIST	PCI-DSS	CES[17]
SO 18 Disaster recovery capabilities	●	●	●	●	●	●	●	●	
SO 19 Monitoring and logging policies	●	●	●		●	●	●	●	●
SO 20 System tests	●		●		●	●	●	●	●
SO 21 Security assessments	●	●	●		●	●		●	●
SO 22 Compliance	●	●	●		●	●			
SO 23 Security of data at rest	●	●	●	●	●	●	●	●	●
SO 24 Interface security		●	●		●	●		●	●
SO 25 - Software security		●	●		●	●	●	●	
SO 26 Interoperability and portability		●	●		●	●			
SO 27 Customer monitoring and log access	●	●	●	●	●	●	●	●	●

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

TP-05-16-077-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-203-5
DOI: 10.2824/456345