NATIONAL CYBERSECURITY FRAMEWORK

Portuguese National Cybersecurity Centre

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

NATIONAL CYBERSECURITY FRAMEWORK

Portuguese National Cybersecurity Centre

Version 1.0 EN
April 2020

1 Foreword

Our country's public and private organizations digital security is a top priority. An adequate maturity level in cybersecurity for these organizations will enable the necessary conditions for an effective and sustainable economic development. For this purpose, preventive measures, in particular, implementing best practices, are of utmost importance and represent a fundamental contribution for this outcome.

The Portuguese National Cybersecurity Centre summed up a set of well known Cybersecurity international accepted standards to develop a **National Cybersecurity Framework,** which allows organizations to perform a risk-based approach to tackle cyber threats, establishing the foundations for the implementation, on a voluntary basis, of security measures for networks and information systems. For that purpose, specific measures have been identified and structured around the following five Cybersecurity objectives: identification, protection, detection, response and recover phases for handling cybersecurity incidents, including the necessary organizational environment to cope with them.

With a simple and clear structure, this document provides guidance for decision makers and IT departments . We invite all the community to adopt this **National Cybersecurity Framework**, and thus contribute both to a better national cybersecurity and, ultimately, to a sustainable economic development.

____

António Gameiro Marques
National Security Authority

____

Lino Santos
Head of National Cybersecurity Centre

INDEX

2 Executive Summary

Organizational awareness of information security has never been more relevant than it is today. There is a growing number of devices connected to the internet, some of them misconfigured or poorly protected, representing a major threat to assets in organizations.

Cybersecurity, in all its components, is a central concern in today's society. A secure environment is fundamental for establishing and developing any economic and social activity. Nowadays, information security is the core of any organization's activity since most of those are done on the digital domain.

In line with the Law 46/2018, of the 13th of August, which establishes the national legal framework for cyberspace security, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, aims to provide a **cybersecurity guide** that, in a comprehensive manner, organizes a set of measures for today's most relevant challenges organizations face in this area. Moreover, it is intended to provide the basis to achieve a **minimum set of the recommended information security** requirements.

Knowing that organizations can be at different maturity levels and have different sizes (ranging from micro and small organizations to medium and large companies or public institutions), and that some recommendations may be either disproportionately demanding considering the size of the organization or not sufficiently demanding, the current document should be used with a critical approach by each organization and adapted according to each context of application.

The document is structured on a set of security measures that highlight the following five specific objectives: **Identify**, **Protect**, **Detect**, **Respond** and **Recover**.

There are references of examples and guidelines that allow the systematization of processes and procedures for the fulfillment of these objectives. The examples and guidelines are not in the form of a checklist with actions to be performed, as they represent key objectives that can be recognized by the parties involved, based on a set of international references and different technical standards.

Objectives are split into categories and subcategories. For each subcategory, this document references examples of technological and procedural implementations, and also identifies samples of evidences, consisting of a generic description of how international references and different technical standard scan be applied, thus contributing to a better understanding of what is required.

This document concludes with a set of additional recommendations, for organizations to be able to comply with legislation on this subject, and also to be prepared, **to manage risk** and **mitigate the impact of incidents** that may affect them through the definition of a strategy that involves the organization as a whole.

Introduction

3.1 Overview

A significant part of our economy, as well as social activities and welfare, are embodied in infrastructures and services available in cyberspace. In this document, cyberspace is understood as a complex environment of values and interests, materialized in an area of collective responsibility, that results from the interaction between people, networks and information systems. This complex and heterogeneous environment offers new possibilities and opportunities but it also creates new threats and a risk environment that can lead to the occurrence of incidents with economic and social impacts that can not be underestimated.

These information technology security incidents may not only impact the cyberspace environment, but can also extend its reach to physical infrastructures that support critical or essential services which support the daily functioning of our society.

In this digital era, many infrastructures operate on the premise that technology elements are robust and reliable and that emerging and complex technologies (for example: *IoT, Cloud Computing, Big Data*) have the potential to offer high flexibility and efficiency in the communication and coordination of services and processes. But this increasing use of information technologies also means that they become more **vulnerable** to illicit and malicious activity and poorly planned operational maintenance processes.

TERRORISTS
CRIMINALS
ACTIVISTS
FOREIGN NATIONS

Figure 1 - Parties Involved Underlying Malicious Activity

The motivations underlying malicious activities, that may be fulfilled by **terrorists**, **criminals**, **activists** or **foreign nations**, are varied. The impact of an incident differs across a wide spectrum with different degrees of severity, ranging from the unavailability of an institutional site with possible reputational impact, to the decrease of a country's defense capability, financial or even human life losses.

From another perspective, proper management of cybersecurity incident risks can also provide opportunities for improving the quality of services offered through the adoption of new practices, development of new products or goods and enhancement of the organization’s reputation.

In 2016, the Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, was approved, focusing on measures to **ensure a high common level of network and information system security** across the European Union (NIS Directive). The NIS Directive aims to ensure that essential service operators and digital service providers take the most adequate and proportionate technical and organizational measures to manage the risks related with network security and information systems used at the operational level. And, also, to ensure that competent authorities or CSIRTs (Computer Security Incident Response Team) are notified without undue delay of incidents with a relevant impact on the continuity of the essential services the organizations provide.

The NIS Directive had as objective to create a legal framework for Member States in the field of cybersecurity legislation and to provide the basis for developing a **cybersecuri-**

ty culture in vital sectors of the economy and the proper functioning of society sectors, which rely on networks and information systems. The Annex II of this Directive supports the following sectors of essential service operators: energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructures. Annex III focuses on the following digital service providers: cloud computing services, online marketing services and online search engine services.

However, we still **lack appropriate approaches** that support and facilitate a rapid and effective cooperation between essential services and digital service providers, both in terms of exchanging specific information regarding incidents or in terms of sharing risk and threat information. In addition, there is a shortfall in capturing and correlating events and information associated with cyber attacks on infrastructures and, also, the existing tools do not provide adequate technical guidance to incident response professionals on how to detect, investigate and reproduce attacks.

Despite the socioeconomic importance of the tools and techniques to deal with incidents, there isn´t an easy, structured, standardized and reliable way to manage and predict interrelated cybersecurity incidents taking into account the heterogeneity and complexity of the incident and the increasingly sophisticated types of attacks. Therefore, there is an **urgent need to create new systems** for efficient incident handling and to support the complete and common understanding of cyber attack situations in a timely manner.

The threats to cyberspace, as potential incidents, should not undermine all the benefits that networks and information systems bring to our society. Responding to a threat or incident should not only be viewed from the perspective of a particular digital service being unavailable, but should also be systematic and focused on the prevention and awareness of all parties involved, whether or not they are citizens, public and private organizations, or the country in general.

The National Cybersecurity Framework, henceforth referred to as NCF-PT, is intended to be a tool available for the society to support this systematic response, which is aligned with the Law 46/2018 (that establishes the national legal framework for cyberspace security, transposing the NIS Directive).

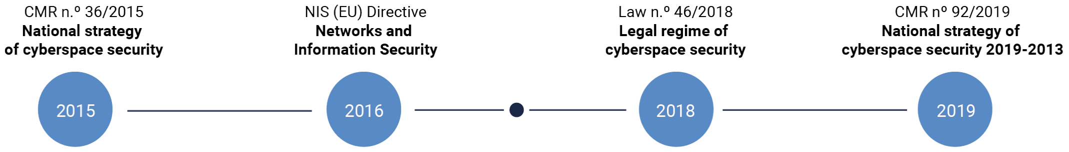
CMR n.º 36/2015
National strategy of cyberspace security
2015
NIS (EU) Directive
Networks and Information Security
2016
Law n.º 46/2018
Legal regime of cyberspace security
2018
CMR nº 92/2019
National strategy of cyberspace security 2019-2013
2019

Figure 2- Chronological Framework

Additionally, the NCF-PT complies with the National Cyberspace Security Strategy, approved by the Council of Ministers Resolution 92/2019, of 23 of May 2019[1] . **The Strategy is based on the commitment to deepening network and information security as a way of guaranteeing the protection and defense of the cyberspace of national interest and enhancing the free, safe and efficient use of it by all citizens, businesses and other public and private entities**. The Strategy is based on three principles, which NCF-PT intends to address as follows:

[1] https://dre.pt/application/conteudo/122498962

a. Subsidiarity: The NCF-PT aims to be a cross-cutting tool for all cyberspace organizations, from private to public operators, responsible for ensuring sovereignty and constitutional principles;
b. Complementarity: Being cross-cutting, the NCF-PT proposes a set of broad and integrative measures that aim to raise awareness among all parties involved in cyberspace and the position they occupy in it;
c. Proportionality: In the NCF-PT, within the security objectives, the adaptation of measures is proposed to the organization, regarding its applicability, size, sector of activity and characterization of the identified risks.

Having a holistic view of both people and infrastructure equipment dedicated to security and be able to follow the proposed measures in the NCF-PT requires an investment in three pillars. First, in creating the figure of the Chief Information Security Officer (**CISO**), as the ultimate responsible for information security within the organization; second, by setting up a Security Operation Centre (**SOC**), to provide the organization the necessary facilities and support teams; third, by setting up a specialized incident response team that can operate on the premises of the SOC, i.e. the creation of the Cybersecurity Incident Response Team (**CSIRT**) function. To clarify these three pillars and their importance in organizations, additional recommendations are provided in the last chapter of the document.

3.2 Objectives

The context of the cybersecurity threat must be addressed through a systematic approach for the awareness of public and private organizations on cybersecurity issues.

For this objective the definition of guidelines for a system of processes and procedures serves to build a necessary paradigm shift on technological and social aspects. These guidelines can be a common language across the different activity sectors that promotes the convergence of the best practices leading to implement cybersecurity in organizations.

The NCF-PT embodies a homogeneous and inclusive view of the Portuguese organizational reality (public and private) regarding the need for the identification, protection, detection, response and recovery measures on threats that jeopardize the **security of its networks and information systems** and, consequently, the information hold.

This document is not a mandatory cybersecurity standard, so it can be used as a reference of identified existing standards, norms and best practices used in information security domains. Thus the application of this document by organizations is voluntary and adaptable to address the specific needs of different sectors, organization sizes and any other distinctive features.

The core structure of the NCF-PT has been defined from an organization's **cybersecurity management lifecycle perspective**, taking into account human, technological and procedural aspects, with a particular focus on risk management processes and procedures.

An intrinsic feature of risk is that it cannot be completely eliminated, making it essential to have an overall organizational strategy to ensure an effective risk management process.

This is an ongoing process of **identification**, **diagnosis** and **response** in which organizations must understand the likelihood of a particular event occurrence (as well as their potential adverse impacts and existing vulnerabilities) in order for a risk to be managed. Based on this approach, any organization can determine its acceptable level of risk as condition for prioritizing cybersecurity activities and thereby ensure the resilience of its activity as provider of goods or services.

3.3 Document Structure

This document’s initial part contains an introduction to NCF-PT, identifying its objectives, context, applicability and definitions. The topic of risk management is also explained, because the understanding of risk is considered necessary for the application of the NCF-PT.

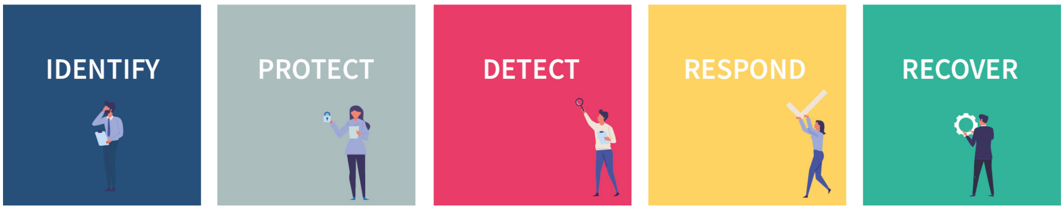

Figure 3- Security Objectives

The chapter “Presentation of the National Cybersecurity Framework” presents the objectives of the NCF-PT: **Identify**, **Protect**, **Detect**, **Respond**, **Recover**. These objectives are organized in thematic categories and subcategories, where technical and procedural measures are explained, as well as the evidence of implementation that enables organizations to improve their ability to protect and respond to cyberspace and information security challenges.

The document concludes, presenting the role of the CISO, with whom the lifecycle management of information security and cybersecurity issues should be addressed. The document also approaches the CSIRT (Computer Security Incident Response Team) and the SOC (Security Operations Centre), their objectives, constitution and also the importance of sharing information about cyber security incidents with the organization's stakeholders.

3.4 Definitions and Abbreviations

3.4.1 Definitions

The following table provides the terms used throughout the document. Whenever applicable, the terms of the current national laws or norms are used. The “Reference” column indicates the respective norm or legislation where the term is defined. Whenever a term is defined in the scope of the NCF-PT, the “Reference” column will show the same abbreviation.

TERMS	DEFINITIONS	REFERENCE
Activity	Process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services.	ISO/IEC 22301
Asset	Item, thing or entity that has potential or actual value to an organization.	ISO/IEC 22000
Availability	Property of being accessible and usable upon demand by an authorized entity.	ISO/IEC 27000
Business continuity	Organization’s capability to continue the delivery of products or services at acceptable predefined levels, following a disruptive incident.	ISO/IEC 22301
Business continuity plan	Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.	ISO/IEC 22301
Cloud computing service	A digital service that provides access to a scalable and adaptable pool of shareable computing resources.	Law 46/2018
Confidentiality	Property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO/IEC 27000
Continual improvement	Recurring activity to enhance performance.	ISO/IEC 9000
Continuous delivery	Approach to the software engineering process, where code or package is produced in short cycles, allowing a consistent delivery and fast iteration cycle.	NCF-PT
Continuous Integration	The practice of automating the integration of code changes from multiple contributors into a single software project.	NCF-PT
Critical asset	An asset that supports, at least, one essential service.	NCF-PT
Critical Infrastructure	A component, system or part thereof, situated in national territory, which is essential for the maintenance of vital functions of society, health, security and economic or social welfare. The disruption or destruction of it would have a significant impact, given the inability to continue to perform its functions.	Law 46/2018
Critical Infrastructure operator	A public or private entity that operates a critical infrastructure.	Law 46/2018
Critical service	A service that supports key processes of an organization.	NCF-PT

TERMS	DEFINITIONS	REFERENCE
Cybercrime	Facts related to crimes defined in the Cybercrime Law and also other criminal offenses committed using technological means, in which these means are essential to the practice of the concerned crime.	ENSC
Cyberdefense	Activity that aims to ensure national defense in or through the cyberspace.	ENSC
Cybersecurity	Set of prevention, monitoring, detection, reaction, analysis and correction measures and actions that are aimed to maintain the desired security state and to ensure the confidentiality, integrity, availability and non-repudiation of networks and information systems in cyberspace, and of the people who interact in it.	ENSC
Cyberspace	Complex environment of values and interests that is materialized in an area of collective responsibility, which results from the interaction between people, networks and information systems.	ENSC
Cyclic redundancy check	An error detection method commonly used in digital networks and storage devices in order to detect accidental change or corruption in data.	NCF-PT
Demilitarized zone	Perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks.	ISO/IEC 27033
Digital service	A service of the information society that is provided at a distance by electronic means.	Law 46/2018
Digital service provider	A legal person that provides a digital service.	Law 46/2018
Document	Information and its supporting medium (for example: paper, digital, magnetic, storage device, photo or reference sample).	ISO/IEC 22301
Domain name services service provider	An entity that provides internet Domain Name Services (DNS) service.	Law 46/2018
Domain Name System (DNS)	A hierarchically distributed naming system in a network that forwards domain name lookups.	Law 46/2018
Essential service	An essential service for the maintenance of crucial societal or economic activities, that depends on networks and information systems, and for which the occurrence of an incident may have relevant disruptive effects on the provisioning of such a service.	Law 46/2018
Essential service operator	A public or private entity that provides an essential service.	Law 46/2018
Exercise	Process to train for, assess, practice, and improve performance in an organization.	ISO/IEC 22301
Framework	Reference model and set of best practices.	ISO/IEC 27001
Hamming codes	Family of linear error-correcting codes. Hamming codes can detect up to two-bit errors or correct one-bit errors without detection of uncorrected errors.	NCF-PT

TERMS	DEFINITIONS	REFERENCE
Honeypot	A computer security mechanism set to detect, deflect or, in some manner, counteract attempts of unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site, but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked.	NCF-PT
Incident	An event with a real adverse effect on the security of networks and information systems.	Law 46/2018
Incident handling	All procedures to support detection, analysis, containment and response to an incident.	Law 46/2018
Integrity	Property of accuracy and completeness.	ISO/IEC 27000
Internet	Collection of interconnected networks in the public domain.	ISO/IEC 27032
Internet Exchange Point	A network structure that allows the interconnection of more than two autonomous independent systems, with the aim to facilitate the exchange of internet traffic.	Law 46/2018
IT Security Incident Response Team	The team that acts by reference to a defined user community, representing an organization, providing a set of security services that includes, namely, network and information system security incident handling and response service.	Law 46/2018
Legacy System	Obsolete system (software or hardware) that remains operational in the organization.	NCF-PT
Management system	A set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives.	ISO/IEC 22301
Networks and Information Systems	Any device or set of devices interconnected or associated, in which one or more develops, through the execution of a program, the automatic processing of informatic data, as well as the electronic communication network, which supports the communication between them and the informatic data set that are stored, treated, recovered or transmitted by the device, having in mind it functioning, use, protection and maintenance.	Law 46/2018
Networks and information systems security	The ability of networks and information systems to resist, with a given level of confidence, to actions that compromise the confidentiality, integrity, availability, authenticity and non-repudiation of stored, transmitted or processed data, or even related services, that are offered by such networks or information systems, or accessible through them.	Law 46/2018
Norm	A technical specification, approved by a recognized standardization body for the repeated or continuous application, whose observance is not mandatory.	Law 46/2018
Online e-commerce services	A digital service that allows consumers or merchants to conclude sales contracts or service provided either on the online website, or on the merchants' website that uses computing services made available in the online market.	Law 46/2018

TERMS	DEFINITIONS	REFERENCE
Online search engine	A digital service that allows users to browse all websites, or websites in a particular language, based on a search on any subject that provides links where information related to the requested content can be found.	Law 46/2018
Organization	A person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.	ISO/IEC 22301
Policy	Intentions and direction of an organization as formally expressed by its top management.	ISO/IEC 22301
Procedure	Specified way to carry out an activity or a process.	ISO/ISO22301
Process	A set of interrelated or interacting activities which transforms inputs into outputs.	ISO/IEC ISO22301
Record	Statement of results achieved or evidence of activities performed.	ISO/IEC 22301
Representative	Any natural or legal person established in the Union, explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT, instead of the digital service provider, with regard to the obligations of that digital service provider under this Directive.	NIS 2016/1148
Risk	A reasonably identifiable circumstance or event with a potential adverse effect on the security of networks and information systems.	Law 46/2018
Risk acceptance	Decision to agree to the further existence of a residual risk after risk treatment.	Council Decision 2013/488/EU
Risk management	Coordinated activities to direct and control an organization concerning to the risk.	ISO/IEC 22301
Risk tolerance	Organization's or interested party's readiness to bear the risk after risk treatment in order to achieve its objectives.	ISO/IEC 22300
Service level agreement	Documented agreement between the organization and the customer that identifies services and their agreed performance.	ISO/IEC 20000
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. This can be an individual or group that has an interest in any decision or activity of an organization.	ISO/IEC 22301
Supplier	An organization that provides a product or a service.	ISO/IEC 9000
Technical specification	A document that defines the technical requirements that a product, process, service or system must fulfill.	Law 46/2018
Threat	Potential cause of an unwanted incident, which may result in harm to a system or organization.	ISO/IEC 27032
Top domain name registration	An entity that manages and operates the Internet domain name registration of a specific top-level domain.	Law 46/2018
Top management	A person or group of people who directs and controls an organization at the highest level.	ISO/IEC 22301
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.	ISO/IEC 27032

Table 1 – Definitions

3.4.2 Abbreviations

ABREVIATIONS	DEFINITIONS
HVAC	Heating, ventilation, and air conditioning.
CCTV	Closed-circuit television.
CD	Continuous Delivery.
CI	Continuous Integration.
CIS	Center for Internet Security.
CISO	Chief Information Security Officer.
COBIT	Control Objectives for Information and Related Technologies.
COO	Chief Operations Officer.
CRC	Cyclic Redundancy Check.
CSC	Critical Security Controls.
CSIRT	Computer Security Incident Response Team.
CVE	Common Vulnerabilities and Exposures.
DLP	Data Loss Prevention.
DMZ	Demilitarized Zone.
DNS	Domain Name System.
ENSC	*Estratégia Nacional de Segurança do Ciberespaço 2019-2023* – National Cyberspace Security Strategy 2019-2023.
IDS	Intrusion Detection System.
IoT	Internet of Things.
IP	Internet Protocol.
IPS	Intrusion Prevention System.
ISACA	Information Systems Audit and Control Association.
ISO	International Organization for Standardization.
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission.
IT	Information Technology.
MITRE	MITRE Corporation, not-for-profit company that maintains CVE database.
NIS	Network and Information Security directive.
NIST	National Institute of Standards and Technology.
NCF-PT	Portuguese National Cybersecurity Framework
RACI	Responsible, Accountable, Consulted and Informed. Responsibility assignment matrix.
SOC	Security Operations Centre.
SWOT	Strengths, Weaknesses, Opportunities, Threats.
VPN	Virtual Private Network.
ISMS	Information Security Management System.
UPS	Uninterruptible Power Source.
WAF	Web Application Firewall.
WWW	World Wide Web.

Tabel 2 - Abbreviations

3.5 Risk Management

3.5.1 Introduction

The NCF-PT proposes a risk-oriented procedural implementation, that enables informed and prioritized decision-making by organizations, in the cybersecurity context. These decisions should always be equally oriented towards ensuring confidentiality, availability and integrity in the provision of the goods or services for a particular organization. In this context, risk is understood as an identifiable circumstance or event, with a potential adverse effect on the security of networks and information systems.

Several approaches are proposed for the process of periodic risk evaluation and assessment of how they relate to the provision of a good or a service. The result of these evaluations should allow the organization to characterize the current situation, define goals and list a set of actions that promote a positive evolution of its situation in the context of cybersecurity. Thus, the NCF-PT allows, for those who apply it, to choose and direct over time the desired improvements in risk management.

Risk management, when carried out systematically and with an improvement logic, is a practice that allows organizations to identify, quantify and establish the priorities against risk acceptance criteria and relevant goals to the organization.

An organization's risk management can be understood as the managing of uncertainty and the determination of the required actions, so that it can be minimized to deemed levels. It is a systematic exercise in which the organization identifies potential threats that may arise from asset vulnerabilities, as well as the associated risk levels, assessing the likelihood of occurrence and possible impacts.

The ISO/IEC 31000[1] provides a set of risk management principles and guidelines for organizations. On the other hand, the ISO/IEC 27005[2] specifies guidelines and processes for managing the security risk of an organization's information systems, relying in particular on the requirements of an Information Security Management System (ISMS) implemented in accordance with ISO/IEC 27001[3].

The ISO/IEC 27005 does not provide a specific methodology for managing information security risks. It is the organization responsibility to define their approach toward risk management. In general, the ISO/IEC 27005 risk management methodology, being directed to information systems, can be applicable to all types of organizations.

The information security primary concern is the protection of the organization's assets against internal and external threats, which are categorized according to the potential damage they may cause to the protected assets.

In the security domain, greater attention is given to threats related to malicious or human activities. The figure below, taken from ISO/IEC 27032[4], illustrates these concepts and high-level relationships.

[1] NP ISO/IEC 31000 – Risk Managemnet – Guidelines

[2] ISO/IEC 27005 – Information Technology – Security techniques – Information Security Risk Management

[3] NP ISO/IEC 27001 – Information Technology – Security techniques – Information Security Management System – Requirements

[4] ISO/IEC 27032 – Information Technology – Security techniques – Guidelines for Cybersecurity

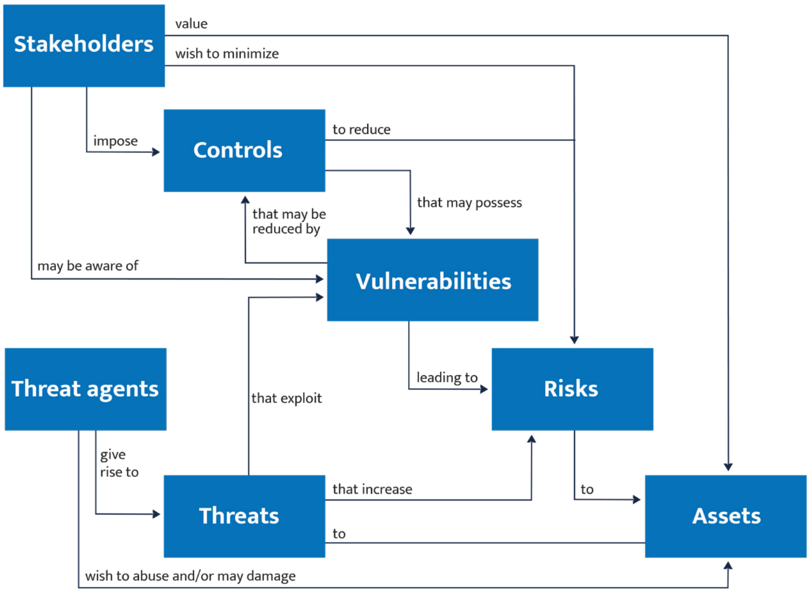

Figure 4 - Source: ISO/IEC 27032, Basic concepts and high level relationships

As it will be explained later in this chapter, the risk management plan is implemented based on the organization's evaluation of identified risks within the analysis process. There are four options available for risk management: Avoid, Accept, Mitigate, and Transfer.

For all the risks in which mitigation has been the treatment option, the organization shall develop a treatment plan that identifies constraints and possible dependencies, current organizational priorities, lead times, required resources and the critical path of mitigation measures implementation.

The procedural and technical measures to be implemented may be identified based on the NCF-PT and the risk framework, and should also aim to reduce the level of risk so that it can be considered acceptable by the organization.

3.5.2 Overview

As observed from the following figure, Information Security Risk Management based on the ISO/IEC 27005 standard consists of the following phases: Establishing the Context (1), Risk Assessment (2), which includes identification (2.1), analysis (2.2) and risk evaluation (2.3), risk treatment (3), risk acceptance (4) followed by the communication and consultation (5) and risk monitoring and review (6).

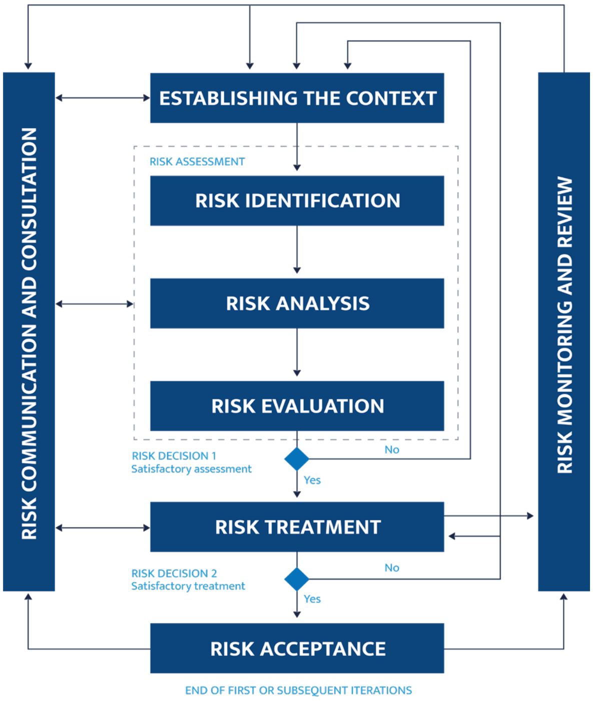

Figure 5 - Source: ISO/IEC 27005, Risk management phases

In this chapter, we will densify each of the indicated phases following the guidelines of ISO/IEC27005 standard, culminating with a practical example of risk management.

3.5.3 Establishing Context

Risk management organization

The organization shall identify which human and material resources are required to ensure the correct execution of the entire risk management process. The organization shall:

- Define a risk management methodology that is appropriate to the reality of the organization;
- Identify internal and external stakeholders;
- Identify the governance model to be applied in risk management and define an appropriate escalation process;
- Define internal and external risk management roles and responsibilities and assign them to eligible human resources. Some examples of these roles are:
    - Risk manager – Responsible element in the risk management process;

    - Risk management team member – Participant element in the risk management process. It may be an asset manager, department officer or a representative of a relevant stakeholder.

- Identify a tool to support risk management and treatment;

- Define and identify which records to create and maintain (for example: meeting minutes, risk analysis monitoring plan, progress reports).

All these decisions must be reviewed and approved by the top management of the organization.

Risk management approach

Following the previous point, the organization should identify the needed resources in order to:

- Be able to define and implement policies, processes and procedures, in the context of risk management and treatment;

- Be able to perform the risk assessment and risk treatment plan;

- Be able to monitor the implemented controls;

- Be able to follow up the effectiveness of the implementation of the risk treatment plan.

Risk evaluation criteria

Risk evaluation criteria should be identified to assess the relevance of risk in the organization, considering:

- The strategic value of related processes to the activity of the organization;
- The criticality of the involved information assets;
- The operational and commercial importance in terms of confidentiality, integrity and availability of the information;
- The expectation and perceptions of the stakeholders.

Additional evaluation criteria that can support the prioritization of risk treatment may be identified.

Impact criteria

The organization shall define the levels of impact that should support its risk management. The impact criteria should be determined in terms of the degree of damage or cost that an information security event has to the organization.

When identifying the impact levels to be assigned to the risks, the organization shall take into account the following indicators:

- The relevance and classification of the information assets;
- Information security breaches, assessed in terms of confidentiality, integrity and availability of information;
- Costs to the organization;
- Disruption of plans and deadlines;
- Reputation damage.

Risk acceptance criteria

The organization shall define its risk acceptance criteria. It should identify from what level of risk it will be necessary to guarantee the top management approval before the risk can be accepted.

The organization shall define its own risk acceptance level scales. When defining risk acceptance criteria, the organization shall consider the following points:

- The acceptance criteria may include several limits, being defined a maximum acceptable risk level. The risk acceptance above that level must be formally approved by top management;

- The acceptance criteria may include requirements for additional future treatment. For example, the risk can be accepted if there is approval and commitment to take steps to reduce it to acceptable levels within a timeframe agreed and stipulated in the risk management group;

- The acceptance criteria may differ according to their lifespan. For example, the risk may be associated with a temporary or short-term activity of the organization.

The acceptance criteria should be established considering the following factors:

- Inherent factors to the activity;
- Operational factors;
- Technological factors;
- Financial factors;
- Social and humanitarian factors.

Scope and boundaries definition

The organization should define the scope and boundaries of its security and information risk management system. The definition of the scope is relevant considering that it is necessary to ensure that all relevant assets to the organization are included in the survey phase.

The definition of border points is important so that the organization is able to address the risks that can be identified across those same borders.

In defining the scope or the boundaries of risk management, the organization should take into account:

- Strategic business goals;
- Processes referring to its activity;
- Functions and internal structure;
- Information security policy;
- Stakeholders' expectations;
- Socio-cultural environment;
- Information assets.

Examples of scope definition for a risk management process can be:

- Building / Location;
- Infrastructure platform;
- Application platform;
- Processes regarding the activity of the organization.

What is not included in the scope should be formally justified by the organization.

3.5.4 Risk identification

The first phase of the risk assessment step is the identification phase. At this stage, the risks that may create constraints or prevent the organization from achieving its goals should be identified, recognized and described.

The purpose of identification is to determine occurrences that may cause a potential loss to the organization. The steps described in the next phases are essential to collect data to feed the risk analysis.

Asset Identification

The organization shall identify which assets support the scope defined in information security risk management. Assets are everything that has value and requires protection from the organization's perspective.

Assets may include (but not limited to) the following categories:

- Technological (hardware, software);
- Network devices;
- People;
- Locations (etc.).

The organization must have an inventory of its assets with, at least:

- The inventory number of the asset;
- A description of their functions;
- The identification of the asset accountable;
- Its location;
- Category or type.

This information should be complemented with:

- Classification of the asset according to its criticality to the organization;
- Identification of processes related to the activity of the organization and that is supported by those assets;
- Identification of dependencies with other assets.

Identify threats

A threat has the potential to have negative impacts and consequences on an organization's assets. Additionally, this threat may be of natural or human origin and may be accidental or deliberate.

The information related to threat identification can be obtained in the following ways:

- Review of the occurred incidents;
- Responsible(s) for the asset;

- Users;
- Information security specialists;
- Physical security specialists;
- Legal Departments;
- Threat catalogs.

The experience gained by the organization in managing and learning from past incidents and threat assessments should be taken into account in the current risk assessment.

It may be relevant for the organization to consult other catalogues (possibly specific to its area of expertise) to complete the generic threat list.

Identify controls

The organization shall have systematized the previous risk management plans with the identification of the respective implemented controls. In addition to this information, is the identification of the status of the controls implementation and usage.

For the identification of existing or planned controls, the following activities may be useful for the organization:

- Review documents containing information about controls implementation (for example: previous risk management processes implementation plans). If information security management processes are properly documented, all planned and/or existing controls and their implementation status should be available for analysis;
- Verification with the persons responsible for information security (for example: CISO, COO) about which controls have actually been implemented;
- Conducting an on-site evaluation to assess the implementation of physical controls, comparing those that are properly implemented against the list of controls that should exist and, verifying among those implemented, whether they are correctly and effectively operationalized.

At the end of this activity, the organization should have a list of all the existing and planned controls with their respective implementation status.

Vulnerability identification

Based on the list of threats and assets (not forgetting the implemented controls), the organization should identify a list of potential vulnerabilities that could be associated with its assets. Vulnerabilities may be identified in the following areas:

- Organization;
- Processes and procedures;
- Management routines;
- Collaborators;
- Physical environment;
- Configuration of information systems;
- Hardware, software and network devices;
- External stakeholders dependencies.

The existence of a vulnerability does not cause any harm by itself. In order for damage to occur, it must exist a threat that can exploit that same vulnerability.

A vulnerability may not require the implementation of a control, but it must be known and monitored by the organization. Please note that a control or a set of controls that are incorrectly implemented, can result in potential vulnerabilities for the organization. The effectiveness of a control depends on the environment in which it is operating.

The organization can identify a complementary list of vulnerabilities that are not related to threats and/or concrete assets. This list may be part of its risk management knowledge database.

Impact identification

The organization must identify the consequences of the risks and assess which will be the impact that a possible manipulation of a vulnerability by a threat may have in terms of confidentiality, integrity and/or availability of assets that are within the scope of the risk management process.

An impact must be assessed in various dimensions, including (but not limited to) the generation of adverse operating conditions, loss of business by the organization or damage of reputation and image.

This activity identifies the damages or impacts to the organization that may be caused by an incident scenario. An incident scenario can be caused by the manipulation of a vulnerability by a certain threat or by a set of threats to an information system.

The impact of incident scenarios should be determined by considering the weighting criteria that are defined while setting the context. A particular threat can impact one or more assets, or parts of assets.

Assets must be classified according to their value to the organization, depending on the consequences on its business in case they are damaged and/or compromised. The impact can be temporary or permanent (as in the case of the destruction of an asset).

The impact of the risk should be identified based on the associated vulnerabilities and threats. Attention should also be given, when identifying the impact, on the consequences to the assets and, inevitably, to the processes relating to the activities of the organization that they support.

In impact assessment, the organization may identify potential operational consequences in terms of, but not limited to:

- Investigation and repair time;
- Work time lost;
- Missed opportunities;
- Security and safety;
- Financial repair costs;
- Reputation damage.

3.5.5 Risk analysis

Risk analysis involves the consideration of uncertainties, sources of risk, consequences, events, scenarios, controls and their effectiveness.

An event can have multiple causes and consequences, and can affect one or more organizational goals. The approach to the risk analysis process may be performed with different levels of granularity, depending on the criticality of the assets and the extent of existing vulnerabilities, the threats to have under consideration and the incidents that have occurred before, that involved the organization and that are within the scope and boundaries of the risk management process.

In the criteria of measuring the risk impact, the following dimensions shall also be observed:

- Reputation - The occurrence of a particular risk may undermine the reputation of the organization (for example: loss of trust by stakeholders);

- Legal or Regulatory - The occurrence of a particular risk may endanger the organization's legal and/or regulatory responsibilities (for example: sectoral regulatory responsibilities);

- Customer Service - The occurrence of a certain risk may jeopardize the service provided to the organization's customers (for example: non-compliance with a service level);

- Financial - The occurrence of a particular event may lead into the incurrence of unforeseen financial costs (for example: fines, additional resources).

The probability of occurrence of a risk is the possibility of it to occur in a certain time period. It is possible for a risk to be identified, based on the sensitivity of the team, the experience of the identifier and/or other internal and external indicators.

Analysis Methodology

The risk analysis methodology can be substantiated by a qualitative or quantitative analytical approach or through the combination of both. In practice, qualitative analysis is best used as a first approach for obtaining general risk level indicators and for identifying the most relevant risks.

The method of analysis shall be consistent with the risk assessment criteria defined in the risk contextual phase.

Qualitative Risk Analysis

Qualitative risk analysis uses a grading qualification scale to identify the severity of potential impacts (for example: Low, Medium and High) and the probability of such occurrences. An advantage of the qualitative analysis is that it is of easy understanding by the participants, despite the disadvantage identified by the subjectivity of the scale in question.

Qualitative risks can be used:

- As an initial screening activity to identify risks that require further analysis;
- When this type of analysis is appropriate for decision making;
- When data or numerical resources are inadequate for a quantitative risk analysis.

Qualitative analysis should use factual data and information.

Quantitative risk analysis

Quantitative analysis uses a numerical value grading scale (as opposed to the descriptive scales used in qualitative risk analysis) to measure impacts and probabilities. It should be supported by a variety of sources.

The quality of analysis depends on the accuracy and integrity of the numerical values and the validity of the used models. Quantitative risk analysis uses, in most cases, incident historical data and, thus, has the advantage that it can be directly related to the organization's information security goals and concerns.

Quantitative analysis may be a disadvantage if no factual and/or auditable data is available. This may create an illusion of the accuracy and effectiveness of the risk assessment process.

Impact survey

To carry out this phase, the organization shall have a list of relevant incident scenarios, the identification of previously analyzed threats and vulnerabilities, the affected assets and the respective consequences for those assets and to the processes regarding the activity of the organization, within the scope of the risk management process.

The impact at the level of services provided by the organization that may result in security incidents should be evaluated. Impact assessment should be evaluated in the context of the loss of confidentiality, integrity and/or availability of the assets under analysis.

The risk impact should be based on vulnerabilities, identified threats and the respective consequences of risk in the assets and processes related to the activity of the organization.

The impact can be assessed from several perspectives, namely, technical, financial, human, image, or from another perspective not mentioned, but relevant to the organization.

The asset evaluation begins with their classification, according to their importance to the achievement of the business objectives of the organization. It can be determined by using two measures:

- The replacement value of the asset: The cost of retrieving, cleaning or replacing information (if possible);
- The operational consequences of loss or impairment of an asset, such as negative consequences for the provision of the service, legal or regulatory consequences resulting from the unavailability and/or destruction of information assets.

Probability analysis

Based on existing threats, vulnerabilities, and incident lists (including lessons learnt), the organization should evaluate what is the likelihood of the risk to occur.

Once incident scenarios including threat identification are identified, affected assets, exploited vulnerabilities, and the impact on the organization's activity and processes assessed, it should be taken into account the frequency of threat events and how easily vulnerabilities could be exploited, considering:

- Experience and statistics applicable to the possibility of threat;
- For human threat sources: the motivation and capabilities that change over time and the available resources to a potential attacker, as well as the perceived attractiveness and vulnerability of assets to a potential attacker;
- For accidental threat sources: geographical factors, such as proximity to chemical or oil industries, the possibility of climatic conditions;
- Vulnerabilities, individually or in combination.

Risk level determination

In the risk analysis, a value is assigned to the impact and likelihood of each identified scenario. These values may be qualitative or quantitative depending on the methodology used by the organization.

At this stage, all the identified risks should have their level defined.

3.5.6 Risk evaluation

The nature of the decisions regarding the evaluation and to the risk evaluation criteria used to make those decisions, are established at the time of context definition. These decisions, as well as the context, should be revisited in more detail at this stage, given that there is more information on the specific identified risks.

Throughout the evaluation process, organizations should compare the estimated risks with the risk assessment criteria defined during the context definition process.

Risk evaluation criteria should be used to support decision making. They should be consistent with the external and internal context of the information security risk management, for example, in the organizations' objectives and stakeholders vision.

The decisions made in the risk evaluation are mainly based on the risk acceptable level. However, impacts and the likelihood, as well as the degree of confidence in risk identification and analysis, should also be considered.

The aggregation of several risks, low or medium, may result in higher overall risks. In the evaluation phase, a list of the risks that can be grouped should be drawn up. Risks should be prioritized according to the evaluation criteria and in relation to the incident scenarios that originated the identified risks.

3.5.7 Risk treatment

In the scope of risk treatment, the organization shall define which treatment option is deemed appropriate. The organization shall identify the controls that can be implemented to mitigate, avoid or transfer the risk, as well as define a treatment plan for it. In choosing risk treatment options, the following should be considered:

- How the risk is perceived by affected stakeholders;
- The most appropriate way to communicate with stakeholders.

Once the risk treatment plan is defined, residual risks should be determined. This process involves updating or re-iterating the evaluation phase, based on the expected effects of the proposed risk treatment.

If the residual risk does not yet meet the organization's risk acceptance criteria, an additional iteration of the risk treatment may be required before it can be accepted.

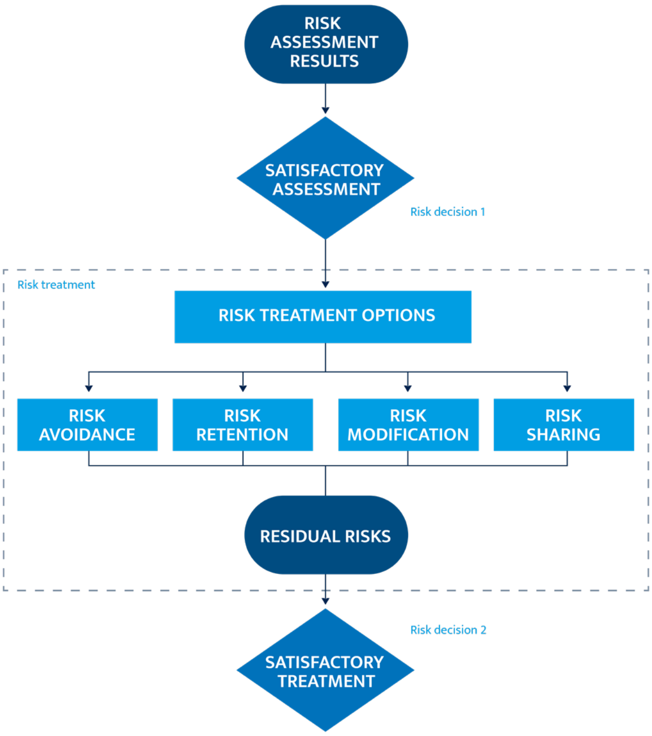

Figure 6 - Source: ISO/IEC 27005, Risk Treatment

As indicated in Figure 6, the risk treatment options to consider are:

- Avoid the risk: Placing the probability or impact tending towards zero, making it more difficult to occur and/or completely eliminating its impact;
- Accept the risk : Risk acceptance decision. The assumption of responsibility for such a decision should be formally registered by the organization;
- Mitigate the risk: Reduce the likelihood and/or impact of an adverse event to acceptable limits by implementing controls or countermeasures;
- Transfer the risk: Transfer, fully or partially, to third parties, the impact in relation to a threat (for example: contract an insurance).

3.5.8 Risk communication and consultation

Information and decisions related to risks should be shared with all relevant stakeholders. Risk communication should be carried out in order to:

- Provide assurance of the outcome of the organization's risk management;
- Collect risk information;
- Share the results of the risk evaluation and present the risk treatment plan;
- Avoid or reduce the occurrence and the impact of information security breaches due to lack of mutual understanding between decision makers and stakeholders;
- Support decision making;
- Enhance knowledge about information security issues in the organization;
- Coordinate with other stakeholders and plan responses in order to reduce the impact of incidents;
- Provide a demonstration of responsibility for the risks to the decision-makers and stakeholders of the organization;
- Improve awareness regarding the importance of the risk management process.

The organization shall develop communication plans to support common and emergency risk management processes. Thus, the communication activity must be carried out continuously.

3.5.9 Risk monitoring and review

Risks and their factors (for example: asset value, impacts, vulnerabilities, and likelihood of occurrence) should be regularly monitored and reviewed, so that any changes, that may have occurred in the context of the organization that could have resulted in a change in risk perception, have been identified in a timely manner.

The organization shall ensure that the following points are continuously monitored:

- New assets that have been included in the risk management process;
- Changes in the criticality of assets to the organization (for example: due to changed business requirements);
- New threats that may be active, both inside and outside the organization, and that have not been yet evaluated;
- Possibility of new vulnerabilities being exploited by threats;
- Possible increase of the impact, consequences of threats, vulnerabilities or grouped risks, that result in an unacceptable level of risk;
- Information security incidents that may occur.

The outcome of monitoring activities may be incorporated into other risk review activities. The organization should perform the review on a regular basis or whenever significant changes occur.

3.5.10 Example

John, the head of the organization's Project Management Office, has identified in his risk analysis process that there is a high possibility of compromise of the user passwords in the file sharing platform. The platform is stored in a cloud computing service, and it is used by the organization to make available all the documentation generated under the scope of the execution of its projects.

The risk identified by John was based on:

- His experience with the platform indicates that his provider does not have a password policy that is aligned with their internal practices;
- The knowledge that another platform client has been the target of a malicious attack.

During the process, he identified that the threat could actually be originated from an external malicious attack, by exploiting the previously identified vulnerability (defective password policy) and he also noted that this attack vector could undermine the confidentiality and integrity of the information stored in this asset (file sharing platform).

John performed the impact assessment based on the systematized matrix of the organization's risk methodology (1 - Small, 2 - Moderate, 3 - High, 4 - Catastrophic), having assigned a “4 - Catastrophic” impact to the identified risk.

Next, he then performed the risk evaluation exercise of the likelihood of the risk occurring. He consulted the methodology and considering the possibilities presented (1 - Unlikely, 2 - Probable, 3 - Very Probable, 4 - Almost Certain), and then decided that the likelihood should be "4 - Almost Certain".

Based on the impact and likelihood calculation, the risk level (result from the product between impact and likelihood) is 16. Thus, John concluded that the identified risk is Very High. This conclusion was supported by the risk level identification criteria that was published under the organization's risk management methodology:

a. [1; 2] – Low Level;
b. [3 a 6] – Medium Level;
c. [8 a 12] – High Level ;
d. [16] – Very High Level.

Given the identified level, the organization cannot accept it, because all "Very High" risks must be dealt with, unless they have been formally accepted by the organization Top Management. In this case, the organization, in its risk assessment, may make the strategic decision to mitigate it and to perform the following activities:

1 Ensure that the file management platform supplier changes their password management policy in accordance with the organization internal practices, within the time frame to be defined;

2 To evaluate other platforms that provide the same service, under conditions deemed appropriate by the organization.

A responsible person (Isabel - Director of Information Systems) for the implementation activities was identified and an estimated resolution date was also agreed upon. The date was chosen according to the priorities assigned to the identified risks, considering the level of risk and the criticality of the assets involved.

All this information has been updated in the organization's risk management tool.

Summary Table

FIELDS	VALUES
#ID	1
Risk Description	Possibility of unauthorized access to the organization projects information
Asset	File Management Platform
Risk Owner	John – Head of Project Management Office
Threat	Malicious password "brute force" attack
Vulnerability	Inadequate password policy
Confidentiality	Yes
Integrity	Yes
Availability	No
Impact	4 – Catastrophic
Likelihood	4 – Almost Certain
Risk Level	16 – Very High
Strategy	Mitigate/Treat

Actions	- Ensure that the file management platform supplier changes their password management policy in accordance with the organization internal practices, within the time frame to be defined; - To evaluate other platforms that provide the same service, under conditions deemed appropriate by the organization.
Responsible for the treatment of the actions	Isabel – Head of Information Systems
Date of treatment	DD-MM-YYYY

Table 3 - Risk Resume

3.6 Scope and Applicability

The NCF-PT has applicability in all national public and private organizations, namely:

1. Public administration;
2. Critical infrastructure operators;
3. Essential service operators;
4. Digital service providers;
5. Any other organizations using information networks and systems.

Otherwise, the NCF-PT may be applied by digital service providers that have their main establishment in the national territory or, in other way, they may appoint a representative based in the national territory, as long as they provide digital services here.

An organization should use the NCF-PT as a support tool for the cybersecurity risk management process. Not being designed to replace existing processes, it can be used in order to complement these same processes, allowing gaps to be identified in the cybersecurity strategy and promoting the definition of a future improvement path.

There are several approaches to the implementation of the NCF-PT. Among them, we highlight the following:

Review of cybersecurity practices

The NCF-PT core structure systematizes an essential set of security measures that can be used to compare with the cybersecurity measures put into practise by the organization. This allows the creation of a current profile and measure the degree of compliance with the requirements described in categories and subcategories, properly aligned with security objectives: Identify, Protect, Detect, Respond and Recover.

An organization may, among other things, acknowledge that they are at a maturity level that allows it to achieve the desired results and focus on the risk monitoring and management process. Alternatively, the organization can identify opportunities or needs to improve their processes. On the other hand, the organization may use this information to identify underinvestment areas and thus prioritize and redirect their resources.

Systematization of processes or improvement of existing ones

The following steps illustrate, not exhaustively, a methodology that can be used by the organization to create a cybersecurity program or make improvements to the existing one based on the NCF-PT. Each of these steps should be repeated as necessary, in order to create a continuous improvement dynamic in the information security and cybersecurity processes and procedures.

Step 1 - Priority and Scope: The organization identifies its high level goals and priorities. Based on this information, the organization defines its strategic options regarding the implementation of cybersecurity measures and defines which universe of systems and assets support the critical activity of the organization. The NCF-PT may be adapted to the various realities of the organization regarding its activity and also considering the different requirements of its internal processes, which may have different levels of risk tolerance.

Step 2 - Guidelines: Once the scope of the cybersecurity program has been defined, the organization identifies and defines information networks and systems and their activity-related assets, regulatory requirements and the risk management strategy. Additionally, the organization identifies threats and vulnerabilities applicable to previously defined assets.

Step 3 – Creation of Current Profile: The organization creates its “Current Profile”, indicating for each category and subcategory which security goals are currently met. If some of the goals are partially met, this situation should be documented, to substantiate the level of maturity and background information for future assessment.

Step 4 - Risk Analysis: Risk analysis can be guided according to the organization's existing risk management process, or based on previous actions. The organization analyzes its operating environment to assess the likelihood of an event or a cybersecurity incident to occur, and its impact on the organization. This process should take into account internal and external sources of information, regarding emerging vulnerabilities and threats, in order to gain a better understanding of the expected likelihood and impact.

Step 5 – Creation of Target Profile: The organization creates its “Target Profile” based on the categories and subcategories described in the NCF-PT, reflecting those which are the intended outcomes. The organization may define its own categories and subcategories, in order to better address the particular characteristics of its activity’s risks. On the other hand, the organization may also consider contributions and requirements from external stakeholders, such as other industry entities and suppliers.

Step 6 - Identify, analyze and prioritize gaps: The organization compares the “Current Profile” with the “Target Profile” and identifies existing gaps that should be addressed. To achieve this, it draws up an action plan that reflects the relevance, costs, benefits and associated risks of the identified gaps, and projects the actions to be taken in place to achieve the results defined in the “Target Profile”.

Step 7 – Action Plan implementation: The organization determines which actions are needed to address the gaps identified in the previous step, and adjusts its current cybersecurity practices to meet its “Target Profile”.

Organizations should repeat this process whenever necessary and with a projected and systematized cadence. For example, an organization might define a higher, repeating frequency of **Step 2 - Guidelines**, in order to improve the quality of their risk analysis processes. On the other hand, organizations can monitor the progress and evolution of their maturity level, by periodically updating their “Current Profile” and subsequently comparing it to their “Target Profile”.

Communication of Cybersecurity Requirements

The NCF-PT seeks to provide a common language for communicating requirements among stakeholders who are responsible for providing essential goods or services. This communication is especially important among organizations across the spectrum of a logistics chain. These chains can reach high levels of complexity, that are reflected in an interdependence of resources and processes.

This universe of stakeholders, relevant to the provision of the organization's goods or services, is part of the cybersecurity ecosystem. Considering the established categories and subcategories in the NCF-PT, as well as the defined profiles, the contextual, procedural and semantic mechanisms leading to accessible and easily conducive communication by the ecosystem are identified.

3.7 NCF-PT Structure

As part of the definition of the NCF-PT central structure, all relevant categories, subcategories and controls/references are defined, taking into account (but not limited to) the following principles:

1 Consider all defining aspects of a cybersecurity ecosystem in national organizations, regardless of their size, nature (public or private), criticality or technological orientation;

2 Cover transversally all sectors of activity;

3 Meet the specific and defining characteristics of the country's social and economic fabric;

4 Promote and allow that certain organizations (eg. regulators) can define their NCF-PT application context for their activity/regulated sector.

The central structure of NCF-PT consists of:

1 Security Objectives;

2 Security Measures.

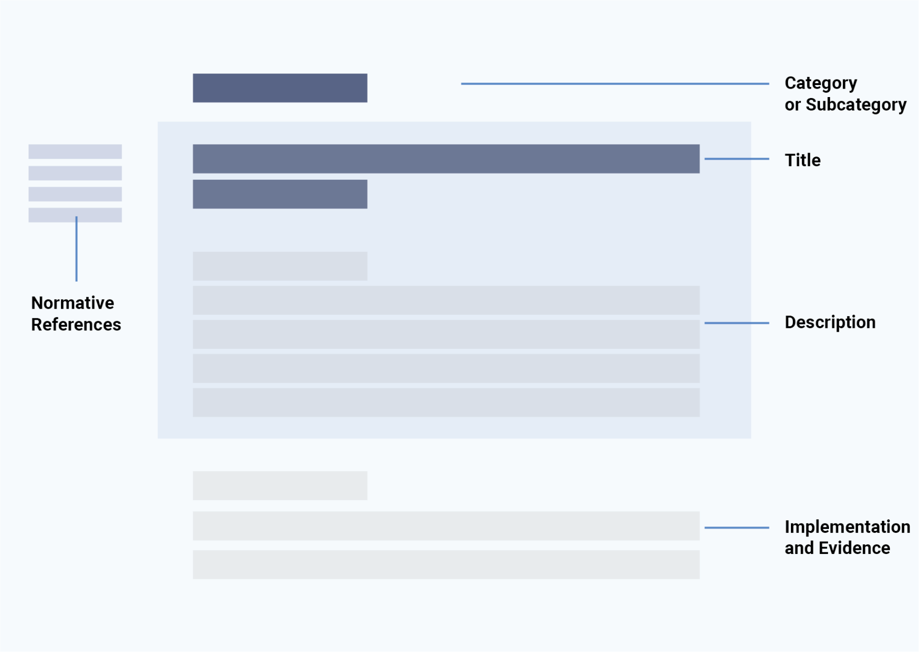

Figure 7 - The document structure

The security measures result in categories that fall into subcategories.

Each security objective can correspond to one or more categories. Each category can correspond to one or more subcategories.

Each subcategory is associated with one or more controls or references. The objective is to connect each of the subcategories to references of best practises in security and cybersecurity, through a set of reference practices of greater acceptance / popularity in Portugal.

For each subcategory, there is a reference to an example of technological implementation and another of procedural implementation, consisting of a generic description of how it can be applied, thereby contributing to a better understanding of its applicability. Generic examples of possible evidence that can be used in demonstrating the application of a certain security measure are also referenced.

The basic structure of the NCF-PT is thus presented:

OBJECTIVE	SECURITY MEASURES					
IDENTIFY	Categories	Subcategories	Technical Implementation	Procedural Implementation	Evidences	Normative References
PROTECT	Categories	Subcategories	Technical Implementation	Procedural Implementation	Evidences	Normative References
DETECT	Categories	Subcategories	Technical Implementation	Procedural Implementation	Evidences	Normative References
RESPOND	Categories	Subcategories	Technical Implementation	Procedural Implementation	Evidences	Normative References
RECOVER	Categories	Subcategories	Technical Implementation	Procedural Implementation	Evidences	Normative References

Table 4 - NCF-PT Base Structure

3.7.1 Reference Context

A context is given below for the four references that support the practices and controls suggested by this NCF-PT. These references address the topic of information security and cybersecurity in a complementary way. All these references are internationally recognized as a basis for the implementation and assessment of risk management controls and of (best) practices for governance, information security and/or cybersecurity.

CIS CSC 7.0

The Critical Security Controls Catalogue (CSC) is published by the Centre for Internet Security(CIS[1]). This catalogue provides a prioritized action list that is regularly reviewed by the academic community in order to be usable by the organizations.

[1] https://www.cisecurity.org

COBIT 5

Under the ISACA[1] responsibility, COBIT is a best practice framework for IT governance. It helps organizations to create value from IT and contributes to balance the benefits, the optimization of risk levels and the use of available resources by organizations.

ISO/IEC 27001:2013

The ISO/IEC 27001[2] standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system, as well as the requirements for security controls to be implemented in accordance with the needs and reality of the organization.

NIST SP-800-53 Rev4

Published by NIST9[3], it is a catalogue of security and privacy controls for government agency networks and information systems. It also provides a process of selecting controls to protect the organization's operations and assets from incidents, natural disasters, structural failures or human error.

3.8 Context

The NCF-PT is intended to be primarily applicable in organizations that are technology based, whether from a perspective of cybersecurity for information technologies, industrial system controls, human machine interface systems, information technology equipment or, more generally, all equipment connected in some way to networks and information systems.

The presented framework is a proposal for a set of information security practices for cybersecurity. It reinforces the fact that, within voluntary application, any organization is free to define what it wants to implement, which security measures to implement or other additional attributes that it may consider relevant, according to its activity type, size and associated risk profile.

Thereafter, we present some situations where the adaptation/application of the NCF-PT in an organization may be justified:

1 A regulator defines the context of application under its sector of activity, selecting subcategories and defining the security measures that they consider appropriate for each subcategory, according to an associated generic risk profile, in their area of activity;

2 An organization makes its own contextualization of the NCF-PT by choosing the subcategories and defining the security measures that fit the risk profile associated with its assets;

3 As a support tool to identify a set of practices that can be implemented by the organization's stakeholders;

[1] https://www.isaca.org/

[2] https://www.iso.org/isolec-27001-information-security.html

[3] https://www.nist.gov/

4 An organization can identify in the NCF-PT possible practices that can be transformed into contractual requirements, intended to improve the exchange relations of goods and services between organizations, framed in the thematic of information security and cybersecurity.

Presentation of the National Cybersecurity Framework

4.1 Security objectives

The NCF-PT provides and describes a set of security measures that translate into specific objectives. Examples and guidelines are referenced, which allows to systematize processes, procedures and tools, whose application allows the achievement of these same goals. The NCF-PT is not a checklist of actions that have to be taken, but rather a representation of the key objectives acknowledged by the various stakeholders as an important support to the cybersecurity risk management process.

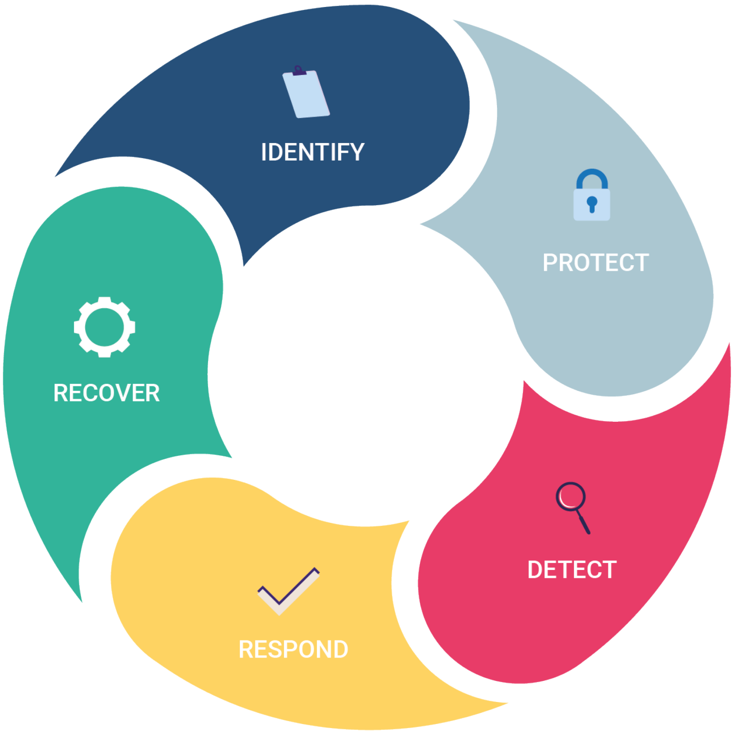

Figure 8- Security Objectives

The application of the NCF-PT should be performed in a continuous improvement perspective. The static use of the practices identified in the NCF-PT should not be performed, but should evolve according to the maturity of the organization and its context.

The following table describes the NCF-PT security objectives:

OBJECTIVE	DESCRIPTION
Identify	Understanding the organization's context, the assets that support the critical business processes and relevant associated risks. Such understanding enables the organization to define and prioritize its resources and investments, according to the risk management strategy and the organization general goals.
Protect	Implementation of measures aimed at protecting the business processes and company assets, regardless of their technological nature. Categories within this function include measures oriented to the protection of the organization in its three dimensions: People, Processes and Technology.
Detect	Definition and implementation of appropriate activities aimed at identifying incidents on time. That is, the detection of events with a real adverse effect on the security of networks and information systems.

OBJECTIVE	DESCRIPTION
Respond	Definition and implementation of appropriate measures in case of incident detection. The proposed measures under this objective are intended to mitigate the impact of the incident, reducing its potential adverse effects.
Recover	Definition and implementation of activities aimed at managing the recovering plans and actions to restore impaired processes and services due to a cybersecurity incident. The aim is to assure the resilience of the organization in its three dimensions: People, Processes and Technology. If an incident occurs, the organization can use the needed actions to support its recovery in an acceptable time.

Table 5 - Security Objectives

4.2 Security measures

In the NCF-PT scope, three basic elements should be considered: Security Measures, Categories and Subcategories.

Security measures are high abstraction activities that support organizations in the process of systematizing their cybersecurity risk management strategy. These measures simplify the process of information organization, risk management decision-making, threat addressing and foster the continuous improvement by resorting to lessons based on accomplished activities.

Additionally, the identified measures are aligned with the most widely adopted incident management methodologies and enable the demonstration of the impact of investment on cybersecurity. For example, the investment in planning and executing exercises that support a timely response and recovery activities, which results in an impact reduction in the provision of goods or services.

A security measure is subdivided into categories that gather programmatic purposes, objectives and particular activities. The categories, in turn, are further divided into subcategories that translate a set of specific effects of a technical or management activity. These results, described non-exhaustively, promote the achievement of the purposes and objectives of the categories in which they fit into.

In the following subchapters, we identify the categories and subcategories corresponding to each security measures.

4.2.1. Identify

An agreement must be established across the organization on the approach to cybersecurity risk management in the context of its networks and information systems, people, assets, data and their capabilities. Practices that fall within the **Identify** objective are fundamental to the effective use of the NCF-PT. In an organizational context, understanding the resources that support its vital functions and their associated risks enable the organization to prioritize its efforts consistently.

The following table describes the NCF-PT **Identify** categories and their associated subcategories.

CATEGORY	DESCRIPTION	SUBCATEGORY
ID.GA **Asset Management**	The organization shall identify the data, personnel, devices, systems and facilities that enable the achievement of its business purposes. These are identified and managed consistently with their relative importance to business goals and the organization's risk strategy.	ID.GA-1 ID.GA-2 ID.GA-3 ID.GA-4 ID.GA-5
ID.AO **Business Environment**	The organization's mission, objectives, stakeholders and activities are understood and prioritized. This information is used to identify cybersecurity roles, responsibilities and support decisions under risk management.	ID.AO-1 ID.AO-2 ID.AO-3 ID.AO-4 ID.AO-5
ID.GV **Governance**	The policies, procedures and processes to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management team of cybersecurity risks.	ID.GV-1 ID.GV-2
ID.AR **Risk Assessment**	The organization understands the cybersecurity risks in the scope of its activities (including mission, functions, image or reputation), organizational assets and people.	ID.AR-1 ID.AR-2 ID.AR-3 ID.AR-4 ID.AR-5
ID.GR **Risk Management Strategy**	The organization's priorities, constraints, risk tolerance and assumptions are established and used to support operational risk decisions.	ID.GR-1 ID.GR-2 ID.GR-3
ID.GL **Supply Chain Risk Management**	Priorities, constraints, risk tolerance levels and assumptions that are used to support decision making in the operational risk management of the supply chain shall be established. The organization shall establish and implement processes to identify, assess and manage risks inherent to the supply chain.	ID.GL-1 ID.GL-2 ID.GL-3 ID.GL-4 ID.GL-5

Table 6 – Identify Category from the Security Measures

4.2.2 Protect

The **Protect** objective aims to the development and implementation of the necessary safeguards, in order to ensure the provision of services or goods, supporting and reinforcing the ability of the organization to limit or avoid the impact of a cybersecurity incident.

This capacity is supported by the management of electronic identity and its respective authorizations, by conducting training and awareness-raising actions and by defining and implementing information protection procedures, processes and technologies.

The following table describes the NCF-PT **Protect** categories and their associated subcategories.

CATEGORY	DESCRIPTION	SUBCATEGORY
PR.GA **Identity Management, authentication and access control**	Access to physical, logical assets and associated facilities shall be limited to authorized users, processes and devices. These should be managed in accordance with the risk assessment of unauthorized access.	PR.GA-1 PR.GA-2 PR.GA-3 PR.GA-4 PR.GA-5 PR.GA-6 PR.GA-7
PR.FC **Awareness and Training**	The organization's personnel and suppliers shall receive cybersecurity awareness education and be adequately trained to perform their information security-related duties and responsibilities, in accordance with the related policies, procedures, and agreements.	PR.FC-1 PR.FC-2 PR.FC-3 PR.FC-4
PR.SD **Data Security**	Information and data shall be managed according with the organization's risk strategy, in order to protect their confidentiality, integrity and availability.	PR.SD-1 PR.SD-2 PR.SD-3 PR.SD-4 PR.SD-5 PR.SD-6 PR.SD-7 PR.SD-8
PR.PI **Information Protection Processes and Procedures**	The security policies, processes and procedures shall be maintained and used to manage the protection of networks and information systems.	PR.PI-1 PR.PI-2 PR.PI-3 PR.PI-4 PR.PI-5 PR.PI-6 PR.PI-7 PR.PI-8 PR.PI-9 PR.PI-10 PR.PI-11 PR.PI-12
PR.MA **Maintenance**	The maintenance and corrections on the networks and information systems shall be carried out in accordance with the existing policies, processes and procedures.	PR.MA-1 PR.MA-2
PR.TP **Protective Technology**	Technical security solutions shall be managed to ensure the confidentiality, integrity and availability of the networks and information systems, in accordance with the related policies, procedures and relevant agreements.	PR.TP-1 PR.TP-2 PR.TP-3 PR.TP-4 PR.TP-5

Table 7 – Protect Category from the Security Measures

4.2.3 Detect

The **Detect** objective aim is to develop appropriate and timely practices for the detection of cybersecurity events, through continuous monitoring of networks and information systems and the implementation of detection processes.

The following table describes the NCF-PT **Detect** categories and their associated subcategories.

CATEGORY	DESCRIPTION	SUBCATEGORY
DE.AE **Anomalies and Events**	Anomalous activity shall be detected in a timely manner and the understanding of the potential impact of events shall be assured.	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5
DE.MC **Security Continuous Monitoring**	The networks and information systems shall be monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.MC-1 DE.MC-2 DE.MC-3 DE.MC-4 DE.MC-5 DE.MC-6 DE.MC-7 DE.MC-8
DE.PD **Detection Processes**	Detection processes and their procedures shall be maintained and tested in order to ensure the recognition of anomalous events.	DE.PD-1 DE.PD-2 DE.PD-3 DE.PD-4 DE.PD-5

Table 8 – Detect Category from the Security Measures

4.2.4 Respond

The **Respond** objective intends the development and implementation of practices that will result in actions to respond to a detected cybersecurity incident. These practices should enable the organization to avoid the impacts of a potential incident, through an incident response planning, communicating with relevant stakeholders, analyzing and mitigating incidents and improving through lessons learnt.

The following table describes the NCF-PT **Respond** categories and their associated subcategories.

CATEGORY	DESCRIPTION	SUBCATEGORY
RS.PR **Response Planning**	Response processes and procedures are executed and maintained to ensure a timely response to detected cybersecurity events.	RS.PR-1
RS.CO **Communications**	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5
RS.AN **Analysis**	Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4 RS.AN-5
RS.MI **Mitigation**	Activities are performed to prevent the expansion of an event, mitigate its effects and eradicate the incidents.	RS.MI-1 RS.MI-2 RS.MI-3
RS.ME **Improvements**	Organizational response activities are improved by incorporating lessons learnt from current and previous detection/response activities.	RS.ME-1 RS.ME-2

Table 9 – Respond Category from the Security Measures

4.2.5 Recover

The **Recover** objective goal is to develop and implement practices and, also, to maintain resilience plans in order to restore any capability and/or service that has been compromised in the sequence of a cybersecurity event.

These practices promote the proper recovery of the organization's operations, in order to reduce the impacts of the occurred incident. Among others, promotes the execution of business continuity and recovery plans, the execution of crisis simulation exercises and promotes plans updates for their continuous improvement.

The following table describes the NCF-PT **Recover** categories and their associated subcategories.

CATEGORY	DESCRIPTION	SUBCATEGORY
RC.PR **Recovery Planning**	Recovery processes and procedures shall be executed and maintained to ensure the recovery of the networks and information systems that were affected by the incidents.	RS.PR-1
RC.ME **Improvements**	Recovery and processes plans shall be improved by incorporating lessons learnt activities resulted from past and current incidents.	RC.ME-1 RC.ME-2
RC.CO **Communications**	Restoration activities are coordinated with internal and external parties, such as coordinating centres, Internet Service Providers, owners of the attacking systems, victims, other CSIRTs and vendors.	RC.CO-1 RC.CO-2

Table 10 – Recovery Category from the Security Measures

SECURITY MEASURES

IDENTIFY

4.3.1 ID.GA Asset Management

N.R. CIS CSC 1; COBIT 5 BAI09.01, BAI09.02;

ISO/IEC 27001:2013 A.8.1.1, A.8.1.2;

NIST SP 800-53 Rev. 4 CM-8, PM-5.

ID.GA-1 - Physical devices and systems within the organization are inventoried

Description

The organization should register its physical devices, networks and information systems, and map them in a structured way. All devices and information systems must be classified according to their importance.

Technical Implementation

1 Asset management tools.

Process Implementation

The following rules should be used to register the organization's devices:

1 Physical devices and systems should be registered in a comprehensive list with, at least, the following details:
   a. Inventory ID;
   b. Equipment name;
   c. Serial number;
   d. Location.

2 Network devices should have the following complementary information:
   a. IP Address;
   b. Hardware Address.

3 Owners should be identified by the following details:
   a. Name;
   b. Direct contact (phone, email);
   c. Department.

4 Physical devices should be classified in accordance with their importance to the organization.

Evidences

1 Updated asset inventory with:
   a. Asset information;
   b. Owners responsible for the active assets;
   c. Classification according to their importance.

N.R. CIS CSC 2; COBIT 5 BAI09.01, BAI09.02, BAI09.05;

ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1;

NIST SP 800-53 Rev. 4 CM-8, PM-5.

ID.GA-2 - Software platforms and applications within the organization are inventoried

Description

Software platforms and applications that support critical services and processes should be classified and inventoried, in accordance with their relevance in the organization's critical processes.

Technical Implementation

1 Asset management tools.

Process Implementation

The organization should create an application inventory, detailing:

1 Relevant technical details;

2 Application owner, with: name, direct contact;

3 The classification of relevance in the organization's critical processes;

4 When applicable, the active support contract type with the software vendor.

Evidences

1 Updated software platforms and application assets inventory, with:
   a. Software platforms and application details;
   b. Owners' information;
   c. Classification of software platforms and applications in accordance with their importance to the organization.

N.R. CIS CSC 2; COBIT 5 DSS05.2;

ISO/IEC 27001:2013 A.13.2.1, A.13.2.2;

NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8.

ID.GA-3 - Organizational communication and data flows are mapped

Description

The organization should have an inventory of the network data flows with all its assigned subnets and mapping of internal and external communication flows. That information is essential for organizations to have a holistic view of the assets that support its communication infrastructure and the existing data flows.

Technical Implementation

1. Asset management tools.

Process Implementation

Organizations should perform the following activities:

1. Inventory network assets;
2. Design the high-level network topology;
3. Define the procedures for information transfers internally and with third parties;
4. Map data flows between its systems and third parties.

Evidences

1. The organization should have:
   a. Inventory entries for the network assets;
   b. List of communication flows, both internal and with relevant third parties;
   c. Information mapping;
   d. Document artifacts that depict the procedures for data transfers.

N.R. COBIT 5 APO02.02, APO10.04, DSS01.02;

ISO/IEC 27001:2013 A.11.2.6;

NIST SP 800-53 Rev. 4 AC-20, SA-9.

ID.GA-4 - External information systems are catalogued

Description

Networks and information systems that are located outside of the organization's facilities should be cataloged to allow the organization to have full knowledge of its assets.

Technical Implementation

1. Asset management tools.

Process Implementation

The organization should have a catalog of its external networks and information systems identifying, at least:

1. Inventory ID;
2. Equipment type;
3. Description;

4 Location;

5 Owner (name, direct contact).

Evidences

1 The organization should have an updated networks and information systems catalog.

N.R. CIS CSC 13, 14;
COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02;
ISO/IEC 27001:2013 A.8.2.1;
NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6.

ID.GA-5 - Resources are prioritized based on their classification, criticality, and business value

Description

The organization should classify its assets (e.g., hardware, devices, data, time, personnel and software), considering the criticality of the processes they are used for. During the inventory process, the organization should:

1 Identify and approve a classification method for assets;

2 Ensure that asset owners classify them accordingly to the internal criticality.

Technical Implementation

1 Asset management tools.

Process Implementation

The organization should ensure:

1 Assets are classified accordingly to the internal criticality for the organization activities they support;

2 Critical assets are nominated.

Evidences

1 Entries in the organization inventory detailing asset criticality.

4.3.2 ID.AO Business Environment

N.R.COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05;

ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2;

NIST SP 800-53 Rev. 4 CP-2, SA-12.

ID.AO-1 - The organization's role in the supply chain is identified and communicated

Description

The organization should be able to identify and classify the suppliers, in the relevant supply chains, considering the services and resources provided under existing contracts.

Technical Implementation

Not applicable.

Process Implementation

The organization should define a supply chain policy that establishes guidelines for engagements, procurement procedures and acceptable behaviors, that should be adopted when dealing with contractors in the supply chain.

After the contracts are signed, the following should be registered:

1 Supplier identification;

2 Scope of the relation with the supplier and the contract;

3 The services contracted:
   a. Essentials and long-term engagements (e.g.: facilities physical security, cleaning, maintenance);
   b. Casuals, for short term engagements (e.g.: printing, small building maintenance, hardware maintenance);

4 The processes, departments and employees that benefit from the services provided by the contractors or suppliers;

5 A single point of contact from the organization that should be responsible to manage the supplier contract and is accountable for the technical performance and behaviors of the contractors or suppliers;

6 The administrative restrictions that might exist (conflicts of interest, contracting ex-employees without vetting from top management, good reputation).

Evidences

1 Documents depicting the supply-chain management policy;

2 Entries in supply-chain inventory of contractors and suppliers.

N.R. COBIT 5 APO02.06, APO03.01;

ISO/IEC 27001:2013 Cláusula 4.1;

NIST SP 800-53 Rev. 4 PM-8.

ID.AO-2 - The organization’s place in critical infrastructure and its industry sector is identified and communicated

Description

The organization should be able to:

1 Identify their role in its industry sector;

2 Identify the relevant third parties, internals and externals, which are relevant for critical services.

Technical Implementation

Not applicable.

Process Implementation

The organization should be able to identify in its information security policy the mission, objectives and relevant third parties.

The organization should perform a SWOT analysis, both in internal and external contexts, which identifies Strengths, Weaknesses, Opportunities and Threats.

Evidences

Information security policy document, including:

1 Vision, mission and objectives for information security;

2 Identification of relevant third parties in the information security context;

3 SWOT analysis.

N.R. COBIT 5 APO02.01, APO02.06, APO03.01;

NIST SP 800-53 Rev. 4 PM-11, SA-14.

ID.AO-3 - Priorities for organizational mission, objectives and activities are established and communicated

Description

The mission, vision, values, strategy and objectives are fundamental for setting up the right guidance for the organization. They provide the positioning inside its activity sector and how it aims to be recognized internally, by its employees, and externally, by clients, suppliers and third party organizations.

Technical Implementation

Not applicable.

Process Implementation

1 Document the mission, vision, value and objectives;

2 Identify relevant parties in the information security context.

Evidences

1 Document supporting the information security policy with vision, mission and objectives of information security.

N.R. COBIT 5 APO10.01, BAI04.02, BAI09.02;

ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3;

NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14.

ID.AO-4 - Dependencies and critical functions for delivery of critical services are established

Description

The organization should ensure the identification and registration of critical assets that are required for the delivery of critical services. The registration should include, at least, the following information:

1 Networks and information systems that support the delivery of critical services, that need protection against energy failure or other disruptions caused by anomalies in the support services;

2 Electric Cabling and/or communication networks that support critical services and require protection against tampering or interception;

3 Capacity planning and monitoring of networks and information systems that support critical services, so it is possible to make educated projections of future needs and aim for resilience against failures and attacks.

Technical Implementation

1 Asset management tools;

2 Software for capacity planning management.

Process Implementation

The organization should perform the identification and record of assets that support critical services, by following the guidelines defined in ID.GA-1, as well as capacity and redundancy planning. Examples:

1 UPS;

2 Dual homing for internet connections;

3 HVAC System;

4 Network ports mapping:
   a. Relation between network ports and devices;
   b. Location.

The organization should implement a monitoring process for capacity management of its critical assets.

Evidences

1 Documents identifying the main assets supporting critical services and their respective capacity;

2 Documents identifying secondary/redundant assets supporting critical services and their respective capacity.

N.R. COBIT 5 BAI03.02, DSS04.02;

ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1;

NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14.

ID.AO-5 - Resilience requirements to support the delivery of critical services are established for all operating states

Description

The organization should identify and define adequate requirements for resilience to support the delivery of critical services.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Identify crisis scenarios;

2 Identify a recovery strategy[1] for facing natural disasters and/or malicious attacks;

3 Define a critical services recovery plan that in the event of a disaster and/or malicious attack, allows the organization to:

   a. Identify activities, durations and requirements for recovering the operation to a normal operating state;

[1] *See ISO/IEC 22301 - Society security - Business continuity management systems - Requirements*

b. Identify the relevant tests for the recovery plan.

Evidences

1 Documents supporting the strategy for protection against natural disasters and malicious attacks;

2 Business continuity strategy support documentation for the organization activities in the context of information security;

3 Documents justifying the capacity planning.

4.3.3 ID.GV Governance

N.R. CIS CSC 19; COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02;

ISO/IEC 27001:2013 A.5.1.1;

NIST SP 800-53 Rev. 4 -1 todos os controlos de segurança.

ID.GV-1 - Organizational cybersecurity policy is established and communicated

Description

The organization should:

1 Define an information security policy;

2 Ensure commitment from top management, for instance, requiring them to approve the policy;

3 Clearly communicate the existence and content of the information security policy to stakeholders.

Technical Implementation

Publish the information security policy in an easy to access repository that all employees can access. Examples:

1 Intranet;

2 Document management system.

Process Implementation

The organization should ensure that its information security policy:

1 Identifies the basis that leads to it;

2 Is formally approved by top management;

3 Is formalized with the stakeholders;

4 Is published in an easy to access repository.

Evidences

1 Document with information security policy;

2 Formal approval stamp by top management;

3 Publishing the information security in digital format, that is easily accessible by all stakeholders;

4 Interviews or formal record stating that each relevant party has received and is aware of the information security policy.

N.R. CIS CSC 19;

COBIT 5 BAI02.01, MEA03.01, MEA03.04;

ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5;

NIST SP 800-53 Rev. 4 -1 todos os controlos de segurança.

ID.GV-2 - Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

Description

The organization should comply with legal and regulatory requirements for cybersecurity, following national and European regulation. Internally, the organization should summarize the legal, regulatory and contractual requirements (national and European) that need to be observed and followed.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Identify in the information security policy the legal and regulatory requirements (both national and European) applicable and the intellectual property protecting guarantees;

2 Create a privacy policy, following the national and European law in force.

Evidences

1 Document listing legal, regulatory and contractual requirements;

2 Audit reports that prove compliance with law and regulation;

3 A privacy policy, that follows the national and European law in force.

4.3.4 ID.AR Risk Assessment

N.R. CIS CSC 4;
COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02;
ISO/IEC 27001:2013 A.12.6.1, A.18.2.3;
NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5.

ID.AR-1 - Asset vulnerabilities are identified and documented

Description

Vulnerability management is the main process organizations should do to assess risk in the information security context. All vulnerabilities that are known and are not yet mitigated or fixed should be evaluated by the organization risk assessment processes and should be formally dealt with. The strategy to mitigate these risks should follow the risk management methodology put in place by the organization.

Technical Implementation

Not applicable.

Process Implementation

The organization should ensure its risk assessment processes includes:

1 An asset vulnerability classification taxonomy for the ones that can be exploitable by possible threats;

2 A record for all known vulnerabilities not yet mitigated or fixed that are identified by its vulnerability management process.

Evidences

1 Support document for risk management;

2 Records of the execution of the risk management process.

N.R. CIS CSC 4;
COBIT 5 BAI08.01;
ISO/IEC 27001:2013 A.6.1.4;
NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16.

ID.AR-2 - Cyber threat intelligence is received from information sharing forums and sources

Description

The organization should establish contact with groups that share information about security concerns and vulnerabilities, to exchange ideas and experience and have access to updated threat intelligence.

Cyber threat intelligence can be gathered from specialty forums or other threat intelligence feeds, such as phishtank or emerging threats.

Technical Implementation

For digital threat intelligence feeds, automatic should be considered, so that collection, cleaning and storage are normalized for further correlation by Security Information and Event Management Systems (SIEM).

Process Implementation

The organization should:

1 Establish contact with information sharing forums and other technical specialists;

2 Have access to:
   a. Vulnerability (and respective fixes and mitigations) databases and distribution lists;
   b. Public or private threat intelligence sources about known threats.

Evidences

1 Structured record of established contacts and relations with sharing forums, distributions lists and technical specialists;

2 Record of external threat intelligence integrations.

N.R. CIS CSC 4; COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04;

ISO/IEC 27001:2013 Cláusula 6.1.2;

NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16.

ID.AR-3 - Both internal and external threats are identified and documented

Description

Under the risk management process scope, the organization should identify and document possible threats that can be used to exploit security vulnerabilities that might be discovered on its assets.

Technical Implementation

Not applicable.

Process Implementation

When performing risk analysis, the organization should identify the threats that can compromise the integrity, confidentiality or availability of its assets.

Evidences

1 Support documents of a risk management methodology;

2 Support record of risk management.

N.R. CIS CSC 4;

COBIT 5 APO12.02;

ISO/IEC 27001:2013 A.12.6.1;

NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16.

ID.AR-4 - Threats, vulnerabilities, likelihoods and impacts are used to determine risk

Description

The organization should identify, in the risk management methodology, what are the criteria for determining probability and risk impact. Those criteria should define how the risk level should be determined. Vulnerabilities and threats should be considered during the risk identification process.

Technical Implementation

Not applicable.

Process Implementation

The risk management methodology should identify the impact levels and probability thresholds that should be considered. These are essential for evaluating the associated risk severity.

Asset value identification is of utmost importance when defining the priorities for risk treatment.

Introducing a math formula for risk level makes the process less subjective and improves the overall quality of evaluations.

Critical factors to account for:

1 Impact;

2 Probability;

3 Asset importance (if relevant).

The organization can establish a set of risk levels[1] for each factor, considering the risk tolerance for a given asset.

The final risk score should be the product of, at least, two of the above factors with custom multipliers. As an example: Impact X Probability or Impact X Probability X Asset Value.

[1] See chapter for risk management

Evidences

1 Supporting documents of a risk management methodology, identifying:
   a. Impact level;
   b. Probability levels;
   c. Asset Value;
   d. Risk score function;

2 Support record for risk management.

N.R. CIS CSC 4;

COBIT 5 APO12.05, APO13.02;

ISO/IEC 27001:2013 Cláusula 6.1.3;

NIST SP 800-53 Rev. 4 PM-4, PM-9.

ID.AR-5 - Risk responses are identified and prioritized

Description

The organization should define an adequate response to the risk level observed. Priority for risk treatment should be defined considering both observed risk and asset value.

Technical Implementation

Not applicable.

Process Implementation

The risk treatment and analysis methodology should include:

1 The strategy for risk response;

2 A definition of strategy prioritization, considering:
   a. Identified risk level;
   b. Asset value.

Evidences

1 Document of a risk management methodology defining the risk response and prioritization;

2 Record for risk management.

4.3.5 ID.GR Risk Management Strategy

N.R. CIS CSC 4;

COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02;ISO/IEC 27001:2013 Cláusula 6.1.3;

ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3;

NIST SP 800-53 Rev. 4 PM-9.

ID.GR-1 - Risk management processes are established and managed

Description

The organization should ensure its risk management process is properly defined and is managed in accordance with previous agreements with stakeholders

Under the risk management scope, the organization should:

1. Define a comprehensive strategy for the management of the risks associated with the operation of computer networks and information systems;
2. Ensure the defined strategy is applied consistently across departments;
3. Name owners for the risk management process;
4. Name owners for risk treatment.

Technical Implementation

The organization should employ risk management information systems.

Process Implementation

1. Define a governance strategy that covers all the risk management lifecycle;
2. Organizational and operations risks in network and Information systems assets must be accounted for;
3. The risk management methodology to choose may be based on ISO/IEC 27005, which guides organizations in the process of identification and definition of information security risk management rules and practices;
4. Organization-wide identification and consistent dissemination of:
   a. Risk tolerance strategy accepted by top management;
   b. Methodologies for defining, evaluating and treating risks;
   c. Methodology for monitoring risk evolution over time.

Evidences

1. Document defining risk identification, evaluation and treatment strategy.

N.R. COBIT 5 APO12.06;

ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3;

NIST SP 800-53 Rev. 4 PM-9.

ID.GR-2 - Organizational risk tolerance is determined and clearly expressed

Description

The organization should define, in the risk management methodology, its strategy for risk treatment, considering the existing risk profiles and correspondent organizational risk tolerance.

Technical Implementation

Not applicable.

Process Implementation

The organization should define in the risk management methodology:

1 The risk tolerance guidance;

2 The top management approval process for risk treatment strategy.

Evidences

1 Support document of a risk management methodology.

N.R. COBIT 5 APO12.02;

ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3;

NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11.

ID.GR-3 - Organizational risk treatment strategy is determined and clearly expressed

Description

The organization should define the risk treatment response to apply to its critical assets, which should consider the organization's risk tolerance and its role in their activity sector.

Technical Implementation

Not applicable.

Process Implementation

The response strategy for critical assets should be identified in the risk management methodology. The response strategy should be one of the following:

1 Avoid – Define the probability and impact scale as being very close to zero, making this choice the most infrequent as possible;

2 Accept – The organization decides to accept the risk. The assumption of responsibility should be formally registered by the organization;

3 Mitigate – Reduce the probability or impact of occurring an adverse event through the implementation of countermeasures;

4 Transfer – Transfer, totally or partially, to third parties, the impact related to the given threat (e.g.: contract insurance).

Evidences

1 Support document of a risk management methodology.

4.3.6 ID.GL Supply Chain Risk Management

N.R. CIS CSC 4; COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02;

ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2;

NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9.

ID.GL-1 - Supply chain risk management processes are identified, established, assessed, managed and agreed to by organizational stakeholders

Description

The organization should audit stakeholders in its supply chain, using the same methodology it uses internally to manage risk.

Technical Implementation

Not applicable.

Process Implementation

The organization should specify in its supply chain management policy:

1 Internal accountable person responsible for performing the risk analysis;

2 Frequency of risk analysis.

Evidences

1 Support document for supply chain risk management.

N.R.COBIT 5

APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03;

ISO/IEC 27001:2013 A.15.2.1, A.15.2.2;

NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9.

ID.GL-2 - Supply chain risks are evaluated

Description

Networks, information system, component and service providers should be identified using the defined process for cyber supply chain management.

The organization should classify its suppliers on:

1 Exposure to privacy/sensitive data;

2 Supply chain impact;

3 Goods and services provided.

Technical Implementation

Not applicable.

Process Implementation

The global classification of suppliers should be done accordingly to the internal supplier management policy. At least, the following details should be recorded:

1 Supplier’s name;

2 Type (category);

3 Importance for provided critical services;

4 Exposure level:
   a. Confidentiality;
   b. Integrity;
   c. Availability.

Evidences

1 Support document for supply chain risk management, defining the rules for classifying suppliers;

2 Record of suppliers and respective categorization.

N.R. COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05;

ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3;

NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9.

ID.GL-3 - Supply chain contracts respect the approved management plan

Description

The organization should ensure that suppliers follow their rules for dealing and securing digital information. Supply chain contracts should include adequate measures to ensure compliance with the objectives defined in the internal information security policy and the plan for supply chain management.

Technical Implementation

Not applicable.

Process Implementation

The organization should ensure its supply chain management policy mandates:

1 Inclusion of confidentiality clauses on established contracts;

2 Signing of Non-Disclosure Agreements with suppliers and their employees.

The confidentiality clauses and NDAs should mandate confidentiality treating information:

1 From the organization;

2 From clients;

3 From other suppliers.

Evidences

1 Support document for supply chain risk management, defining the required contractual clauses for suppliers.

N.R.COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05;

ISO/IEC 27001:2013 A.15.2.1, A.15.2.2;

NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12.

ID.GL-4 - Suppliers and third-party partners are routinely assessed

Description

The organization should implement routine audits, test or other forms of evaluations to confirm suppliers and third-parties are meeting their contractual obligations.

Technical Implementation

Not applicable.

Process Implementation

The organization's supply management policy should define:

1 Supplier audit plan;

2 Audit methods and tests;

3 Monitoring and continuous improvement processes of the provided goods and services by suppliers.

The previous points should be evaluated according to the categorization that the organization defines for suppliers. This categorization should be defined by evaluating the exposure to sensitive or privacy information by suppliers.

Evidences

1 Support document of the supply chain risk management;

2 Suppliers list.

N.R. CIS CSC 19;20;

COBIT 5 DSS04.04;

ISO/IEC 27001:2013 A.17.1.3;

NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9.

ID.GL-5 - Response and recovery planning and testing are conducted with suppliers and third-party providers

Description

The organization should define which suppliers need to participate in their response and recovery plans, to ensure they are engaged in planed tests and exercises.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Identify on the supplier list if their presence is mandatory for recovery and response testing. If so, what the associated plan of engagement is;

2 Record of eligible suppliers' engagement in previous tests or exercises.

Evidences

1 Suppliers list;

2 Report of past exercises and disaster recovery tests.

SECURITY MEASURES

PROTECT

4.4.1 PR.GA Identity Management, Authentication and Access Control

PR.GA-1 - Identities and credentials are issued, managed, verified, revoked and audited

N.R. CIS CSC 1, 5, 15, 16;

COBIT 5 DSS05.04, DSS06.03;

ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3;

NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11.

Description

The organization should ensure identities and credentials are issued, managed, verified, revoked and audited in accordance with established internal processes.

Technical Implementation

1 Information system for identity and access management;

2 Central directory of users and groups;

3 Federated authentication services.

Process Implementation

The organization should create, disseminate, review and update:

1 Identity and access management (IAM) process for relevant assets;

2 Functional profiles and associated accesses;

3 Procedures on how to implement IAM for new accesses.

On the identity and access management system, the organization should:

1 Identify all types of existing accounts by usage type, such as nominal, privileged, service, applicational, temporary and emergency;

2 Define rules and conditions for users to belong to access packages and roles;

3 Define the set of authorized users for each information system;

4 Define the required approvals for requesting a specific access;

5 Create, activate, disable, modify and remove accounts;

6 Notify the access owners:
   a. If an access has become stale;
   b. If the account owner moves to another department or function;
   c. When the account owner leaves the company;
   d. Whenever a situation occurs that requires changes in the functional access for an account owner.

Evidences

1. Support document for account lifecycle management;
2. Access catalog for accessing organization assets;
3. Registration of users in the IAM information system.

N.R. COBIT 5 DSS01.04, DSS05.05;

COBIT 5 DSS04.04;

ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8;

NIST SSP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8.

PR.GA-2 - Physical access to assets is managed and protected

Description

The organization should protect and manage the physical access to its facilities and infrastructures that support its networks and information systems.

This control should be applied to all employees and visitors alike, to organization zones to which access is restricted or to sensitive areas that harbor confidential information, networks or information systems.

Technical Implementation

The organization should:

1. Perform physical access based on magnetic cards (or other authentication mechanism with equivalent characteristics) and install access barriers with tourniquets or security doors in restricted access areas;
2. Ensure the integration of the access control system with the IAM system, having the restricted access areas mapped with a central authorization system;
3. Keep a record of ins and outs of external people with at least the following information: name, company, entry time, exit time, internal escort name and purpose of visit.

Process Implementation

The organization should:

1. Create and keep up to date a list of authorized personnel that can access restricted areas where networks and information systems are located;
2. Issue authorization credentials for specific accesses (e.g.: magnetic cards, one-time passwords);
3. Review and approve access lists and specific authorization credentials with a predefined frequency;

4 Control access to defined restricted security areas by:
   a. Verifying personnel identity prior to entry;
   b. Controlling entry and exit points using physical restriction mechanisms;
   c. Keep an audit log of key passage points;
   d. Ensure visitors are accompanied by authorized personnel;

5 Provide the necessary security controls to ensure access to public zones.

Evidences

1 Audit record of entry and exit time for restricted areas;

2 Physical controls that restrict access to properly authenticated personnel.

PR.GA-3 - Remote access is managed

N.R. CIS CSC 12;

COBIT 5 APO13.01, DSS01.04, DSS05.03;

ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1;

NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15.

Description

The organization should document, manage and control remote access to its networks and information systems.

Remote access consists of all accesses made to network or information systems through external communication networks that are not under the organization’s control. VPNs, when established, should be considered as internal accesses and have, at least, equal security controls.

Access to public information is not considered remote access.

Technical Implementation

1 Identity and access management;

2 Central directory of users;

3 Federated authentication services;

4 Technological solution for remote access.

Process Implementation

The organization should:

1 Document the remote access policy;

2 Document remote work policy;

3 Establish rules and guidelines for remote access usage;

4 Monitor non-authorized accesses;

5 Formally authorize accesses to network and information systems, through remote access, before the final access is granted;

6 Define and ensure the requirements for accessing networks and information systems from remote locations.

Evidences

1 Support document for remote work and remote access policies;

2 Technological solution for remote access.

N.R. CIS CSC 3, 5, 12, 14, 15, 16, 18;

COBIT 5 DSS05.04;

ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5;

NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24.

PR.GA-4 - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

Description

Access permissions and authorizations should be managed incorporating the principles of least privilege and segregation of duties. The principles of least privilege states that the accesses given for networks and information systems should be the strictly necessary for users to perform their activities. The separation of duties state that privileges should be split among multiple individuals, so that sensitive processes can not be executed by a single person.

The main reason to employ separation of duties is the prevention of security incidents that can have an impact on the organization's operational activities. Requiring multiple individuals reduces the opportunity for transgressions and increases the probability of detection and reporting.

Separation of duties can be applied to the following process types:

1 **Sequential**: When activities can be broken down into simpler tasks that can be executed by different people (e.g.: in access granting, one-person requests, another approves, and a third one grant);

2 **Quorum**: When activities require a minimum number of members of a deliberative assembly necessary to conduct the business of that organization (e.g.: recovery of a crypto key where policy required two or more system administrators in agreement);

3 **Geospatial:** When activities can be broken down into tasks that are performed in different physical locations (e.g.: Information system management by remote teams).

Technical Implementation

1 IAM lifecycle management.

Process Implementation

The organization should:

1 Create a mapping of functions by role;

2 Create a mapping of accesses by role;

3 Have in place a formal process for managing the accesses lifecycle;

4 Employ the least privilege principle;

5 Employ separation of duties for critical activities.

Evidences

1 Support documents of an IAM process;

2 Record of IAM for systems and applications by functional role;

3 Separation of duties matrix by functional role and activities.

N.R. CIS CSC 9, 14, 15, 18;

COBIT 5 DSS01.05, DSS05.02;

ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3;

NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7.

PR.GA-5 - Network integrity is protected

Description

The network integrity should be protected by the implementation of network segregation and segmentation.

Network design should not be flat, meaning it should not be possible to access any system from any subnetwork.

Security zones should be defined with clearly stated purposes and well-defined barriers enforced by security equipments (e.g.: routers, gateways, firewalls).

Network segregations should be well documented and supported in policies that establish the governance model, namely, which authorizations are mandatory for approving new flows and which flows between zones are pre-approved.

The information flows between systems should require specific approvals and respect the internal policies.

Examples of flow restrictions:

1 Do not allow clear text traffic with a client or privacy data flowing to the internet;

2 Block ingress traffic from spoofed sources;

3 Block direct access to the internet without going through a corporate proxy;

4 Limit data transfers based on data structures and content.

The flow control should be based on the type of information and the path it is being routed through. Fence control should be employed in perimeter equipment such as routers, firewalls or proxies.

Technical Implementation

1 *Firewall*;

2 Network segregation with specific functions (e.g.: Management, DMZ, Internet, Intranet, etc.).

Process Implementation

The organization should:

1 Create a network segregation norm;

2 Define exclusive subnets with pre-defined functions;

3 Define which communication flows are pre-approved for zone boundary crossing and for each zone;

4 Define and implement the rule change management workflow;

5 Define and implement reviews for legacy or unused flows, with a defined periodicity;

6 Ensure the separation of duties on the several activities for flow rule management;

7 Create a data exchange policy that requires strong encryption;

8 Define the rules for internet access.

Evidences

1 Document with policy for network segregation and security zones;

2 Document with information transfer;

3 Document with network usage policy;

4 Document with network operation procedures;

5 Record with past request and approvals for network flow changes.

N.R. CIS CSC, 16;

COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03;

ISO/IEC 27001:2013, A.7.1.1, A.9.2.1;

NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3.

PR.GA-6 - Identities are proofed and bound to credentials and asserted in interactions

Description

The identities of employees are bound and proofed, they are reviewed often and credential input is interactive when required.

Prior employment verification should be performed within what is permitted by national laws.

Technical Implementation

1 Identity and access management.

Process Implementation

The organization should:

1 Do credential verification and background check new hires, following the national law and taking into consideration the scope of work;

2 Implement a formal process to register new employees (where a unique non-shared credential is bound to a user);

3 Implement a formal process to cancel old employees' credentials;

4 Implement a formal process to manage accesses and identities.

Evidences

1 Record of previous background checks;

2 Support document for IAM processes;

3 Support document for onboarding and offboarding procedures;

4 Audit record for onboarding and offboarding procedures and for IAM procedures.

N.R. CIS CSC 1, 12, 15, 16;

COBIT 5 DSS05.04, DSS05.10, DSS06.10;

ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4;

NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11.

PR.GA-7 - Users, devices and other assets are authenticated commensurate with the risk of the transaction

Description

The authentication mechanisms should be defined and updated commensurate to the systems and role profiles, to ensure information integrity and confidentiality.

Technical Implementation

1 Identity and access management;

2 Directory of users and groups;

3 Federated authentication system;

4 Multiple factor authentication mechanisms.

Process Implementation

The organization should:

1 Create and update a password management policy;

2 Create, maintain and disseminate IAM policy;

3 Implement multiple factor authentication (MFA) for accessing critical assets.

Evidences

1 Support document with password management policy;

2 Support document with IAM policy;

3 Audit reports for MFA systems.

4.4.2 PR.FC Awareness and Training

N.R. CIS CSC 17, 18;

COBIT 5 APO07.03, BAI05.07;

ISO/IEC 27001:2013 A.7.2.2, A.12.2.1;

NIST SP 800-53 Rev. 4 AT-2, PM-13.

PR.FC-1 - All users are informed and trained

Description

The organization should establish a plan of action for training employees on information security. The processes and procedures to ensure proper implementation should be set up and the success of training activities should be monitored.

Technical Implementation

Not applicable.

Process Implementation

The organization should create, disseminate and keep updated:

1. A training plan;
2. Training workshops in information security for relevant stakeholders;
3. Formal processes and procedures to ease up implementation efforts for training;
4. Measure the success of training sessions, by interviewing and questioning participants.

Evidences

1. Training plan in information security;
2. Record of past training sessions and respective participants;
3. Training materials and programmatic contents for scheduled sessions;
4. Results of participants’ interviews and questionnaires.

N.R. CIS CSC 5, 17, 18;

COBIT 5APO07.02, DSS05.04, DSS06.03;

ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;

NIST SP 800-53 Rev. 4 AT-3, PM-13.

PR.FC-2 - Privileged users understand their roles and responsibilities

Description

Employees with privileged credentials for networks or information systems should be thoroughly trained in their functions until they master their roles and responsibilities. The organization is responsible for defining the programmatic content for the required training, ensuring it is effective.

Technical Implementation

Not applicable.

Process Implementation

The organization should provide training sessions about privileged accesses to employees:

1. Before they start executing functions that require these type of accesses;
2. When a significant change on granted accesses occurs;
3. Regularly, with the frequency defined by the organization.

Evidences

1. Training plans for privileged access topics;
2. Training materials (slides, documents, exercises);
3. Record of training sessions and respective participants.

N.R. CIS CSC 17;

COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05;

ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2;

NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16.

PR.FC-3 - Third-party stakeholders understand their roles and responsibilities

Description

Third party stakeholders should understand their roles and responsibilities in the scope of the organization's information security program. This understanding is essential to increase the security level readiness of the organization.

The organizations should perform awareness training sessions for third party stakeholders.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Establish the minimal security requirements, activities and responsibilities that clients and suppliers should adhere to;

2 Audit clients and suppliers to ensure they comply with the defined requirements;

3 Train, raise awareness and audit.

Evidences

1 Document with minimal security requirements for clients and suppliers;

2 Audit reports from clients and/or suppliers stating the compliance level with defined requirements;

3 Records of past awareness sessions.

N.R. CIS CSC 17, 19;

COBIT 5 EDM01.01, APO01.02, APO07.03;

ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;

NIST SP 800-53 Rev. 4 AT-3, PM-13.

PR.FC-4 - Senior executives understand their roles and responsibilities

Description

Top management should be engaged and support information security and cybersecurity. They should be aware of their roles and responsibilities in this topic.

Technical Implementation

Not applicable.

Process Implementation

The organization should ensure that senior executives have:

1 Their roles and responsibilities well defined;

2 Regular training sessions about information security and cybersecurity.

Evidences

1 Roles and responsibilities are well defined;

2 RACI matrix including senior executives;

3 Registers of past training sessions.

4.4.3 PR.SD Data Security

N.R. CIS CSC 13, 14;

COBIT 5APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06;

ISO/IEC 27001:2013 A.8.2.3;

NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28.

PR.SD-1 - Data-at-rest is protected

Description

Networks and information systems should protect the confidentiality and integrity of an organization's data at rest.

Technical Implementation

1. Filesystem, databases and backup encryption services;
2. Cryptographic validation of stored data.

Process Implementation

The organization should ensure:

1. Data is stored according to the confidentiality classification that was defined for it;
2. Rules are established for storing data and documents in the different types of supported devices;
3. Data encryption policy includes protection of data at rest, considering classification and location.

Evidences

1. Support documents for information classification policy;
2. Support documents for data encryption policy;
3. Support documents for data at rest encryption.

N.R. CIS CSC 13, 14;

COBIT 5 APO01.06, DSS05.02, DSS06.06;

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;

NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12.

PR.SD-2 - Data-in-transit is protected

Description

The organization should protect the integrity and confidentiality of data in transit. This control should be applied both to internal and external communications.

For distributed systems, this control should be applied end to end to ensure the integrity between all components and services, from components that generate data to the ones that receive data.

When end to end protection is not possible or practical, the organization should set up compensatory controls or explicitly accept the risk or transfer it to a contractual supplier.

Technical Implementation

1 Network communication encryption services.

Process Implementation

The organization should ensure that:

1 Information transfers are performed in a secure way, following the inplace policies defined for the information classification;

2 Information encryption policy includes data confidentiality and integrity controls for data in transit.

Evidences

1 Support documents for information classification policy;

2 Support documents for data encryption policy;

3 Support documents for data in transit encryption.

N.R. CIS CSC 1;

COBIT 5 BAI09.03;

ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7;

NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16.

PR.SD-3 - Assets are formally managed throughout removal, transfers and disposition

Description

The organization should ensure the existence of procedures for authorization, monitoring, record and control of networks, information systems and devices that go in and out of physical and virtual facilities.

When the information is no longer relevant for the organization, anonymization mechanisms should be applied considering the existing information classification policy.

Technical Implementation

1 Shreading software;

2 Removable devices encryption.

Process Implementation

The organization should:

1 Draft procedures for assets lifecyle management;

2 Draft procedures for data transfer through removable devices.

Evidences

1 Support documents for assets lifecycle management;

2 Support documents for information classification;

3 Audit trails for asset attribution and removal of employees.

PR.SD-4 - Adequate capacity to ensure availability is maintained

N.R. CIS CSC 1, 2, 13;

COBIT 5 APO13.01, BAI04.04;

ISO/IEC 27001:2013 A.12.1.3, A.17.2.1;

NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5.

Description

Network and information system capacity should be monitored. Capacity planning should include future needs based on predictions from past usage, to ensure the system performance is aligned with the requirements for providing critical services.

Technical Implementation

1 Metrics and historical capacity monitoring of IT resources;

2 Implement a network and information system redundancy for assets supporting critical services.

Process Implementation

The organization should:

1 Create procedures for managing three types of primary capacity:
   a. Storage capacity (databases, filesystems, others);
   b. Memory and CPU (computational power);
   c. Network bandwidth and throughput;

2 Be proactive using prevision for future capacity and needs as a motif for improvements;

3 Be proactive in monitoring alerts and improve capacity before degradation of services occur due to resource exhaustion.

Evidences

1 Support documents for the capacity management process;

2 Capacity management reports;

3 Evaluation actions for capacity management reports;

4 Evaluation of redundancy applied to networks and information systems that support critical assets.

N.R. CIS CSC 13,

COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02;

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.10.1.1, A.11.1.4,A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3;

NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4.

PR.SD-5 - Protections against data leaks are implemented

Description

The organization should implement security controls on its facility borders, network perimeters and information systems to detect and mitigate unauthorized data leaks.

The scope and frequency of action should match the associated risk. This risk should be based on the information confidentiality.

Technical Implementation

1 Data loss prevention systems;

2 Email information classification system.

Process Implementation

The organization should:

1 Implement measures to prevent unauthorized data leaks:
   a. Mandatory data formats and protocols;
   b. Monitoring for stenography;
   c. Restrict usage of the external network interface to a strict minimum;
   d. Monitoring headers and flows for network packets;
   e. Perform pattern analysis on network traffic to detect anomalies;

2 Create procedures that make the adoption of information classification rules effective.

Evidences

1 Support documents for acceptable asset use policy;

2 Information classification policy:
   a. Treatment and transport of confidential information;

3 Record of information classification.

N.R. CIS CSC 2, 3;

COBIT 5 APO01.06, BAI06.01, DSS06.02;

ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4;

NIST SP 800-53 Rev. 4 SC-16, SI-7.

PR.SD-6 - Integrity checking mechanisms are used to verify software, firmware, and information integrity

Description

The organization should use verification mechanisms to ensure software, firmware and data integrity. These controls are intended to detect unauthorized tampering or unexpected errors due to misuse.

Technical Implementation

1 Static security analysis;

2 Dynamic security analysis;

3 Interactive security tests for networks and information systems;

4 Integrity validation algorithms (parity, hamming codes, CRC, crypto hashes);

5 Implement a central integrity verification tool.

Process Implementation

The organization should:

1 Define the processes and procedures for quality control that have mandatory integrity checks for software and/or firmware;

2 Define the procedures for data integrity validation;

3 Apply static, dynamic and interactive analysis to source code.

Evidences

1 Support documents for processes and procedures for integrity validation;

2 Reports of past integrity verification executions.

N.R. CIS CSC 18, 20;

COBIT 5 BAI03.08, BAI07.04;

ISO/IEC 27001:2013 A.12.1.4;

NIST SP 800-53 Rev. 4 CM-2.

PR.SD-7 - The development and testing environment(s) are separate from the production environment

Description

The organization should ensure that production, testing and development environments are segregated, either logically or physically.

The development and test environments should be segregated not only in accesses, but on a data level as well.

Technical Implementation

1 Network security zones;

2 Physical or logical environment segregation;

3 Anonymization of production data when transported to testing and development environments.

Process Implementation

The organization should:

1 Create, disseminate and keep updated a policy for secure software development;

2 Protect production environments and their network and information systems from unplanned or unexpected events that may be related to test or development activities;

3 Perform configuration management of environments with different objectives (stability in production, flexibility in development);

4 Anonymize production data prior to copying it to test or development environments;

5 Ensure new software production releases go through a change management process.

Evidences

1 Support documents for secure software development;

2 Support documents for software change management;

3 Record of the execution of change management processes;

4 Record of the segregation of environments.

N.R. COBIT 5 BAI03.05;

ISO/IEC 27001:2013 A.11.2.4;

NIST SP 800-53 Rev. 4 SA-10, SI-7.

PR.SD-8 - Integrity checking mechanisms are used to verify hardware integrity

Description

The organization should ensure the hardware integrity by promoting periodic validations and verifications by the manufacturer or a certified supplier.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Perform hardware maintenance by a vendor or certified supplier.

Evidences

1 Hardware maintenance contracts;

2 Hardware maintenance plans.

4.4.4 PR.PI Information Protection Processes and Procedures

N.R. CIS CSC 3, 9, 11;

COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05;

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;

NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10.

PR.PI-1 - A baseline configuration of information technology/industrial control systems is created and maintained

Description

The organization should establish a base configuration for network and information systems.

Base configuration includes:

1 Software installed in workstations;

2 Personal equipment, laptops, printers and mobile devices;

3 Servers and network elements;

4 Security patches for operating systems and applications;

5 Configurations and default parameters;

6 Network topology and logical network and information systems architectures.

Technical Implementation

1. Continuous integration and continuous delivery system;
2. System for managing software updates.

Process Implementation

The organization should:

1. Develop, document and maintain under version control the current configuration for networks and information systems;
2. Create, document and maintain a security policy for networks and systems that:
    a. Apply the principles of the least privilege;
    b. Authorize, ban and restrict usage of functions, ports, protocols and services deemed insecure.

Evidences

1. Support documents for a secure software development policy;
2. Record of version control usage.

N.R. CIS CSC 18;

COBIT 5 APO13.01, BAI03.01, BAI03.02, BAI03.03;

ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5;

NIST SP 800-53 Rev. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17.

PR.PI-2 - A System Development Life Cycle to manage systems is implemented

Description

The organization should apply the sound engineering principles for information security on the specification, design, development, implementation and change of networks and information systems. These principles should be applied both to new systems and existing systems that are going through significant changes. For legacy systems, these principles should be applied as possible, considering the state of hardware, software and firmware.

Technical Implementation

1. Continuous integration and continuous delivery system;
2. Source code version control tool;
3. Document management about network and information security in an enterprise content management system.

Process Implementation

The organization should:

1 Define the security requirements for software projects;

2 Manage the lifecycle of networks and information systems considering:
   a. Layered protections;
   b. Principles of security by default;
   c. Definition of physical and logical barriers and attack surface areas;
   d. Identification of use cases, threats, attacker profiles, attack vectors and patterns to consider compensatory controls;

3 Define and document roles and responsibilities on the development lifecycle;

4 Identify employees that have the responsibility for ensuring secure software development in the development lifecycle;

5 Integrate risk management information in the development lifecycle.

Evidences

1 Documents with security requirements for software projects;

2 Policy for security software development;

3 Audit of past penetration tests.

PR.PI-3 - Configuration change control processes are in place

N.R. CIS CSC 3, 11;

COBIT 5 BAI01.06, BAI06.01;

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;

NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10.

Description

The organization should implement a formal process for change management.

Technical Implementation

1 Change management systems;

2 Continuous integration and delivery system;

3 Source code version control system.

Process Implementation

The organization should ensure:

1 Networks and information systems configurations are formally reviewed considering the principles of the least functionality and security hardening policies;

2 The creation, documentation and update of the change management procedures that:

a. Specify the types of changes where version control should be mandatory;
b. Identify the assets where changes can have a direct or indirect impact;
c. Defines the process for change approvals and rejections;
d. Documents the testing tasks, tests and recovery tasks as necessary;
e. Documents the decisions made and the changes that were applied;

3 Analysis of network and information systems changes to identify potential security impacts prior to implementation.

Evidences

1 Document with change management process;

2 Audit trails of past changes.

N.R. CIS CSC 10;

COBIT 5 APO13.01, DSS01.01, DSS04.07;

ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3;

NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9.

PR.PI-4 - Backups of information are conducted, maintained and tested

Description

The organizations should ensure backup copies can be restored if needed. They should be regularly tested and validated through the execution of restore tests. These tests can be executed in the scope of the business continuity plan, or through planned regular exercises, and have the purpose of testing the integrity of stored copies.

Technical Implementation

1 Backup tool.

Process Implementation

The organization should:

1 Protect the confidentiality, integrity and availability of backups;
2 Consider storing the backups in a safe place outside its facilities;
3 Perform regular backups of user data, systems and documentation for networks and systems;
4 Regularly test the restore of backups and initiate corrective measures in case of failure.

Evidences

1 Support documents with a backup policy;

2 Audit of past execution and restore of backups;

3 Audit of past tests for backups and restore.

N.R. COBIT 5 DSS01.04, DSS05.05;

ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3;

NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18.

PR.PI-5 - Policy and regulations regarding the operationalization of the physical environments of organizational assets should be followed

Description

The organization should follow the national policies and regulations for protecting networks and information systems against natural disasters, power failures, fires and floods.

Technical Implementation

1 Surge protection;

2 Physical devices to simplify and make the energy control safer;

3 Generator for emergency power;

4 Smoke, humidity, water flood and temperature sensors.

Process Implementation

The organization should:

1 Install smoke, humidity, water flood and temperature sensors in the proper places;

2 Protect emergency systems from unauthorized activations;

3 Provide a failsafe mechanism to disconnect networks and information systems in case of emergency;

4 Perform, within the defined timelines, the proper maintenance of the above emergency systems;

5 Protect cabling from external unauthorized accesses.

Evidences

1 Audit of access controls to physical facilities;

2 Maintenance contracts for emergency systems and devices;

3 Audit of previous maintenances;

4 Audit of business continuity plan tests.

N.R. COBIT 5 BAI09.03, DSS05.06;

ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7;

NIST SP 800-53 Rev. 4 MP-6.

PR.PI-6 - Data is destroyed according to policy

Description

The digital and physical information should be subject to appropriated shredding methods according to their confidentiality classification.

Technical Implementation

1 Shredding of deleted confidential files;

2 Paper shredder.

Process Implementation

1 At the end of the information lifecycle, the organization should implement the controls that ensure its proper destruction, considering the confidentiality classification and respecting the national and sectorial laws;

2 When performed by third parties, the organization should apply additional controls to ensure the effective destruction of information;

3 The organization should apply shredding mechanisms (digital or physical):
  a. Before the elimination of data;
  b. When data is moved outside the organization's control.

Evidences

1 Support document for information classification;

2 Assets lifecycle management process;

3 Audit trails for past data shredding.

N.R. COBIT 5 APO11.06, APO12.06, DSS04.05;

ISO/IEC 27001:2013 A.16.1.6, Cláusula 9, Cláusula 10;

NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6.

PR.PI-7 - Protection processes are improved

Description

The organization should evaluate and regularly update its protection processes so that possible existing vulnerabilities can be identified as a target for a correction plan.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Monitor, analyse, evaluate and audit the performance of controls, process and management systems;

2 Perform internal audits;

3 Define and implement action plans for continuous improvement.

Evidences

1 Reports from previous internal audits;

2 Reports of action plans for continuous improvement;

3 Reports of improvement implementation.

PR.PI-8 - The effectiveness of protection technologies must be taken into account in the improvement of protection processes

N.R. COBIT 5 BAI08.04, DSS03.04;

ISO/IEC 27001:2013 A.16.1.6;

NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4.

Description

The organization should be committed to continuous improvement, performing lessons learned sessions and analyzing past incidents. These lessons have the objective of reducing the risk of occurrence of future incidents of the same type.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Regularly practice the process of lessons learned from past security incidents;

2 Promote knowledge sharing from what was learned from investigating and resolving past incidents;

3 Review and update the incident handling process.

Evidences

1 Records of past improvement actions derived from past incidents;

2 Incident response handling process: effectiveness assessment of protection methods;

3 Lessons learned from incidents: continuous improvement of protection methods;

4 Version updates to the incident handling response plan.

N.R. CIS CSC 19;

COBIT 5 APO12.06, DSS04.03;

ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3;

NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17.

PR.PI-9 - Response plans and recovery plans are in place and managed

Description

The incident response, business continuity, incident handling and disaster recovery plans should be updated regularly.

The organization should ensure that stakeholders, both internal and external, are aware of the updates.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Create a response and recovery incident handling plan that:
   a. Has a response capacity plan for incident handling;
   b. Depicts the organization and structure of the initial response;
   c. Defines what is a security incident;
   d. Defines the required resources for supporting incident handling;
   e. Defines the response procedures to data leaks;

2 Create a business continuity plan that:
   a. Defines scope, roles, responsibilities, senior management engagement and coordination with relevant external stakeholders;
   b. Identifies the essential functions for the good functioning of the organization and the contingency requirement for them;
   c. Defines recovery priorities, objectives and metrics;
   d. Provides guidance for total recovery of essential functions;

3 Disseminate the recovery response plans to all stakeholders;

4 Review the business continuity plans regularly.

Evidences

1 Business continuity plan;

2 Response and recovery plans of security incidents;

3 Reports from previous incident responses and recoveries.

N.R. CIS CSC 19, 20;

COBIT 5 DSS04.04;

ISO/IEC 27001:2013 A.17.1.3;

NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14.

PR.PI-10 - Response and recovery plans are tested

Description

The organization should ensure that security incident handling plans and business continuity plans are tested and evaluated to determine efficiency and possible weak points.

Technical Implementation

Not applicable.

Process Implementation

The organization should perform the following types of testing:

1 Business continuity plans exercises;

2 Real life simulations of disasters;

3 Conformity list verification.

Evidences

1 Reports of the execution of exercises and tests of business continuity and the response and recovery from security incidents.

N.R. CIS CSC 5, 16;

COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05;

ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4;

NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21.

PR.PI-11 - Cybersecurity is included in human resources practices

Description

Organization procedures for human resources, such as candidates triage, contracting, role categorization and termination of employment, should be evaluated and reviewed considering the established security requirements.

Technical Implementation

Not applicable.

Process Implementation

The organization should update the human resources procedures for onboarding, role change and offboarding of employees, by doing:

1 A role categorization in terms of function, scope, responsibilities and risk;

2 Triage of new hires, considering the perceived risk for the role;

3 Triage of existing workers for high risk roles on a regular basis;

4 For movers:
  a. Physical and logical access review of networks and information systems;
  b. Confirm operational needs before ensuring access persistence;
  c. Update accesses considering the requirements of new roles;

5 For leavers:
  a. Cancel all accesses to networks and systems;
  b. Collect all relevant assets in the possession of the former-employee;

In case of non-compliance with the established information security policies, the disciplinary action process should be triggered.

Evidences

1 Support documents for human resources management;

2 Employee book.

N.R. CIS CSC 4, 18, 20;

COBIT 5 BAI03.10, DSS05.01, DSS05.02;

ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3;

NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2.

PR.PI-12 - A vulnerability management plan is developed and implemented

Description

The organization should define and implement a vulnerability management plan for networks and information systems.

Technical Implementation

1 Vulnerability scanning tool.

Process Implementation

The organization should define and implement a vulnerability management plan that:

1 Does regular vulnerability scanning against networks and information systems with:
  a. An execution plan for subnet scanning;
  b. Temporal windows for execution;

c. A detailed report of identified vulnerabilities;

2 Allows for sharing vulnerability reports to relevant stakeholders;

3 Analyses the vulnerability and identification of a response plan;

4 Treats vulnerabilities in alignment with the organization’s risk tolerance, as defined in the methodology for risk management;

5 Can share vulnerability details to technical teams, to help resolve a similar vulnerability on other networks and systems;

6 Can share vulnerability details with external stakeholders depending on the type of vulnerability identified.

Evidences

1 Support document of the vulnerability management process;

2 Reports of past executions of the vulnerability management process;

3 Reports from vulnerability scannings and/or pentests.

4.4.5 PR.MA Maintenance

N.R. COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05;

ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6;

NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6.

PR.MA-1 - Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools

Description

The organization should perform maintenance on its critical assets in a regular and scheduled basis.

Interventions should be registered and performed under the supervision of authorized personnel with proper technical knowledge and credentials.

Technical Implementation

1 Ticket management tool.

Process Implementation

The organization should:

1 Develop, disseminate, review and update the system maintenance process and procedures, defining scope, purpose, roles and responsibilities of all relevant stakeholders;

2 Schedule, plan, execute, document and review maintenance records from interventions on networks and information systems;

3 Establish an authorization process for maintenance personnel and keep a list of vetted individuals;

4 Ensure that individuals that execute maintenance to network and systems have the proper authorizations;

5 Assign internal employees to manage in person the work being done by external individuals;

6 Regularly execute, and within predefined time frames, the maintenance of critical assets.

Evidences

1 Access control deployment in protected areas;

2 Maintenance process of physical devices;

3 Maintenance plans and execution reports;

4 Record of past intervention on the critical assets.

N.R. CIS CSC 3, 5;

COBIT 5 DSS05.04;

ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1;

NIST SP 800-53 Rev. 4 MA-4.

PR.MA-2 - Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access

Description

Remote maintenance of systems and networks should be subject to previous approval processes and registered and executed safely to avoid the occurrence of unauthorized accesses.

Technical Implementation

1 Record of maintenance interventions on the request management system.

Process Implementation

The organization should:

1 Approve and monitor both remote maintenance interventions and diagnostic activities;

2 Use strong authentication mechanisms to establish remote sessions;

3 Keep a record of remote maintenance and diagnostic activities;

4. Ensure connections are terminated when the intervention is finished.

Evidences

1. Support documents for the suppliers maintenance policy;
2. Records of equipment maintenance and warranties;
3. Records of executed interventions and rejections;
4. Signed NDAs with suppliers.

4.4.6 PR.TP Protective Technology

N.R. CIS CSC 1, 3, 5, 6, 14, 15, 16;

COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01;

ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1;

NIST SP 800-53 Rev. 4 família AU.

PR.TP-1 - Audit/log records are documented, implemented and reviewed in accordance with the policies

Description

Audit records are defined, documented, implemented and reviewed following the corresponding policy.

Technical Implementation

1. Security Information and event management;
2. Central log and audit record collection.

Process Implementation

The organization should:

1. Create, disseminate, review and update the SIEM policy;
2. Create, disseminate, review and update the SIEM procedures;
3. Define the types of audit records that networks and information systems should support;
4. Pefine the reasoning to keep audit records for incident analysis;
5. Define what type of events should be recorded and saved;
6. Define the taxonomy for log records (e.g.: When, Where, What, Who, Why);
7. Estimate the local and central storage capacity to store audit/log records and define their retention period;

8 Ensure that audit/log records are time synched, using the same source (NTP) and time zone;

9 Ensure that audit/log records are protected against tampering;

10 Ensure the non-repudiation of the audit and log records.

Evidences

1 Event management policy, audit logs and policies;

2 SIEM implementation.

N.R. CIS CSC 8, 13;

COBIT 5 APO13.01, DSS05.02, DSS05.06;

ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9;

NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8.

PR.TP-2 - Removable media is protected and its use restricted, according to policy

Description

The organization should implement procedures that enforce the rules for using removable media, considering the information classification policy in-place.

Technical Implementation

1 Restrict physical access to removable media (e.g.: security boxes for workstations), removing the insert, reading or writing capacity on that media using software;

2 Encryption management for removable media.

Process Implementation

The organization should:

1 Restrict access to removable media, according to the defined information classification policy;

2 Define the encryption policy that includes removable media;

3 Implement physical or logical controls to enforce the information classification policy in-place;

4 Make available software for shredding and anonymize data, following the information classification policy in-place;

5 Protect and control removable media circulating outside or out of protected areas;

6 Restrict the transport activity to people with the required authorizations.

Evidences

1 Support documents for information classification policy;

2 Support documents for reasonable assets usage;

3 Support documents for information encryption policy.

N.R. CIS CSC 3, 11, 14;

COBIT 5 DSS05.02, DSS05.05, DSS06.06;

ISO/IEC 27001:2013 A.9.1.2;

NIST SP 800-53 Rev. 4 AC-3, CM-7.

PR.TP-3 - The principle of least functionality is incorporated

Description

The organization should incorporate the principle of least functionality by configuring systems to provide only essential capabilities. Also, authorized users should only have access to the functionalities required to perform their tasks according to their functional profile.

Technical Implementation

1 Identity and access management.

Process Implementation

The organization should:

1 Incorporate the principle of least functionality for network and information system tasks by:
  a. Restricting functionalities, ports, protocols and services;
  b. Restricting processes to only perform the required functions;
  c. Restricting the principle of least privileges to comply with the mission of the organization;
  d. Restricting access to security functions;
  e. Restricting network access to privileged commands;
  f. Restricting processing domains;
  g. Restricting usage of privileged accounts;
  h. Restricting privileges for code execution.

Evidences

1 Support documents for IAM processes;

2 Definition of roles, responsibilities and separation of duties;

3 Functional profiles mapped with accesses for applications and systems.

N.R. CIS CSC 8, 12, 15;

COBIT 5 DSS05.02, APO13.01;

ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3;

NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43.

PR.TP-4 - Communications and control networks are protected

Description

The flows regulate the information transfer and the paths that can be open inside systems and between systems. These should be controlled operationally and should always require authorizations before they are changed.

Technical Implementation

1. Intrusion detection and prevention system;
2. Firewall;
3. Proxy;
4. Web application firewall.

The technological components identified above are not exhaustive and, therefore, the organizations can implement additional security controls.

Process Implementation

The organization should ensure:

1. The network changes in communications are executed following the change management process in-place.

Evidences

1. Existence of network devices performing security functions;
2. Records of network segregation;
3. Records of requests of network changes.

N.R. COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05;

ISO/IEC 27001:2013 A.17.1.2, A.17.2.1;

NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6.

PR.TP-5 - Mechanisms are implemented to achieve resilience requirements in normal and adverse situations

Description

The organization should implement the necessary mechanisms to ensure basic resilience in uncommon situations and to maintain the proper allocation of additional resources if needed. If an adverse situation still appears, then the business continuity plan should be activated.

Technical Implementation

1. High availability systems;
2. Load balancers;
3. Redundancy systems.

Process Implementation

The organization should:

1. Define the maximum acceptable downtime for assets supporting critical services;
2. Provide additional resources to recover the equipment that failed;
3. Ensure networks and information systems can work in safe mode, when the pre-defined conditions are detected;
4. Protect the availability of networks and information systems by provisioning the required computational resources and prioritizing systems considering their criticality;
5. Establish an alternate location that ensures the necessary capacity to allow the transfer of networks and information systems required for the execution of the organization’s critical activities, at a level equivalent to the primary work site.

Evidences

1. Support documents to the business continuity plan;
2. Records of implemented redundancies.

SECURITY MEASURES

DETECT

4.5.1 DE.AE Anomalies and Events

N.R. CIS CSC 1, 4, 6, 12, 13, 15, 16;

COBIT 5 DSS03.01;

ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2;

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4.

DE.AE-1 - A baseline of network operations and expected data flows for users and systems is established and managed

Description

The organization should ensure that network operations are executed in a structured way by qualified personnel and that information integrity, confidentiality and availability are protected.

For each information system, the organization should measure, create and maintain a reference model for expected communications, whether these are generated by users or systems (both internal and external).

Technical Implementation

1 Intrusion detection and prevention system;

2 Firewall;

3 Proxy;

4 Web application firewall.

Process Implementation

On the network infrastructure operation, which includes all network and security devices, the organization should:

1 Ensure a reference standard for users and systems data flows;

2 Ensure the reference standard is updated with networks and systems natural evolution;

3 Ensure changes are performed in compliance with the existing change management process.

Evidences

1 Model for registering data flows;

2 Records of the data flow communication matrix for network and information systems;

3 Records of past changes.

N.R. CIS CSC 3, 6, 13, 15;

COBIT 5 DSS05.07;

ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4;

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4.

DE.AE-2 - Detected events are analyzed to understand attack targets and methods

Description

The organizations should implement a SIEM that:

1. Supports the process of analysis and event treatment;
2. Supports the process to identify possible security incidents.

Technical Implementation

1. Security information and event management.

Process Implementation

The organization should:

1. Implement a monitoring process for networks and information systems that allows the analysis of past events;
2. Create a set of processes to perform event management and evaluate if they might require deeper evaluation;
3. Ensure enough information is gathered about detected events that make it possible to identify sources, targets and attack methods;
4. Ensure security incidents are created for relevant events.

Evidences

1. Support documents for SIEM;
2. Support documents for security incident handling;
3. Reports from past incident handling.

N.R. CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16;

COBIT 5 BAI08.02;

ISO/IEC 27001:2013 A.12.4.1, A.16.1.7;

DE.AE-3 - Event data are collected and correlated from multiple sources and sensors

Description

The organization should implement the technological and processual mechanisms that allow the collection and correlation of events generated by networks, information systems and security devices.

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

These events should be correlated between them and, if possible, enriched with external threat intelligence feeds.

Technical Implementation

1 SIEM;

2 Integration of external security threat intelligence;

3 Honeypots, as alert probes (early detection system).

Process Implementation

The organization should:

1 Ensure the collection of security events from network devices, security devices and information systems;

2 Correlate collected events with information from past incidents;

3 Correlate collected events among themselves, to detect anomalies;

4 Correlate collected events with external threat intelligence feeds;

5 Evaluate the relevance to notify and communicate ongoing or past security incidents to authorities, third parties, clients and the public.

Evidences

1 Support documents for SIEM;

2 Records from collecting and correlating events;

3 Deployment of honeypots in the organization's network.

N.R. CIS CSC 4, 6;

COBIT 5 APO12.06, DSS03.01;

ISO/IEC 27001:2013 A.16.1.4;

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4.

DE.AE-4 - The impact of events is determined

Description

The organization should perform the classification and typification of events and evaluate the impact on network information systems.

Event categorization supports the decision process about which actions to perform for each type. Security incidents should be raised for certain events.

Technical Implementation

1 SIEM.

Process Implementation

The SIEM should be complemented with:

1 Event categorization and typification;

2 Impact gauging;

3 Activating the incident handling when needed.

Evidences

1 Support document for SIEM;

2 Support document for event taxonomy;

3 Event typification records;

4 Connection between SIEM and incident cases.

N.R. CIS CSC 6, 19;

COBIT 5 APO12.06, DSS03.01;

ISO/IEC 27001:2013 A.16.1.4;

NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8.

DE.AE-5 - Incident alert thresholds are established

Description

Based on the typification and categorization of SIEM events, the organization should define the criteria that justifies the creation of a new security incident.

Technical Implementation

1 SIEM.

Process Implementation

The organization should:

1 Define incident priority taxonomy;

2 Define the limits for event types, set of event types or correlation of events that justify the creation of a security incident;

3 Define the threshold that raises or decreases the security incident priority.

Evidences

1 Support document for SIEM;

2 Support document for incident handling;

3 Records of past incident categorization and prioritization.

4.5.2 DE.MC Monitoring

N.R. CIS CSC 1, 7, 8, 12, 13, 15, 16;

COBIT 5 DSS01.03, DSS03.05, DSS05.07;

NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4.

DE.MC-1 - The network is monitored to detect potential cybersecurity events

Description

The organization should monitor its networks and information systems. The monitoring process should be integrated and fed into the existing event management process.

Technical Implementation

1 SIEM;

2 Intrusion detection and prevention system;

3 Web application firewall.

Process Implementation

The organization should:

1 Develop a strategy of continuous monitoring of information security and data privacy;

2 Monitor information systems to detect attacks and collect key indicators for past incidents, according to the defined strategy;

3 Monitor network connections to detect unauthorized accesses;

4 Adjust the monitoring level when there is a risk change in assets or individuals;

5 Monitor strategic points to control transactions of interest (e.g.: detect direct http connections on firewalls, without going through approved proxies).

Evidences

1 Support document for SIEM;

2 Support document for incident handling;

3 SIEM;

4 Existence of security devices deployed and active on the organization's network.

N.R. COBIT 5 DSS01.04, DSS01.05;

ISO/IEC 27001:2013 A.11.1.1, A.11.1.2;

NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20.

DE.MC-2 - The physical environment is monitored to detect potential cybersecurity events

Description

The organization should ensure physical security perimeters are monitored. Events from physical control points should be inserted into the SIEM with a specific categorization and typification.

Technical Implementation

1 CCTV / Physical access management system;

2 SIEM.

Process Implementation

The organization should ensure that:

1 The physical security control points generate audit/log record;

2 These events are correlated on the SIEM with other security information;

3 Specific alerts are set up to detect intrusion through non-authorized accesses.

Evidences

1 Support document for SIEM;

2 Audit/log records of physical security control points.

N.R. CIS CSC 5, 7, 14, 16;

COBIT 5 DSS05.07;

ISO/IEC 27001:2013 A.12.4.1, A.12.4.3;

NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11.

DE.MC-3 - Personnel activity is monitored to detect potential cybersecurity events

Description

Employee activity monitoring should be integrated on the scope of event management. This activity should generate enough information to allow quick action when a security event is created through the user's activity.

Legal and regulatory consideration should be given according to which type of information is gathered and treated. The organization's privacy policy should define the guidelines on who to use this information.

Technical Implementation

1 SIEM;

2 Correlate employee activity with normal usage patterns.

Process Implementation

Employee activity monitoring should:

1 Occur in their daily activities, when interacting with network and information systems;

2 Occur when privileged accesses are required;

3 Be correlated with normal usage patterns;

4 Generate security incidents when the appropriate threshold is met;

5 Follow the privacy policy for dealing with personal data.

Evidences

1 Support document for SIEM;

2 Incident alert reports with representative event typification and anomalous behavior of the employees activity.

N.R. CIS CSC 4, 7, 8, 12;

COBIT 5 DSS05.01;

ISO/IEC 27001:2013 A.12.2.1;

NIST SP SP 800-53 Rev. 4 SI-3, SI-8.

DE.MC-4 - Malicious code should be detected

Description

The organization should implement mechanisms that allow the detection of malicious code in its networks and information systems. If possible, aim for prevention against execution.

Technical Implementation

The organization should:

1 Implement detection and prevention mechanisms against malicious code running on its networks and information systems that:
   a. Periodicaly or in real time implement code verification;
   b. Analyse files with external origin (e.g.: downloaded from the internet or copied from removable devices);
   c. Block or quarantine in reponse to malware detection;

2 Implement tools and activities of source code review and dependencies on third party code;

3 Feed events into the existing SIEM.

Process Implementation

The organization should:

1 Ensure that malware detection and prevention mechanisms generate audit/log reports;

2 Ensure that audit/log records are collected and correlated on the existing SIEM;

3 Create specific alerts for malware detection and prevention;

4 Address false positive hits and their potential for disrupting system availability;

5 Analyse malware code and check for patterns that could help detect other variants.

Evidences

1 Support document for secure software development;

2 Support document for SIEM;

3 Malware detection and prevention system;

4 Specific alerts for malware detection.

N.R. CIS CSC 7, 8; COBIT 5 DSS05.01; ISO/IEC 27001:2013 A.12.5.1, A.12.6.2; NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44.

DE.MC-5 - Unauthorized mobile applications are detected

Description

The organization should be able to detect unauthorized applications running on its networks and information systems. These detections should be integrated into the existing SIEM.

Technical Implementation

1. Mobile device managers;
2. SIEM;

Process Implementation

The organization should:

1. Define, document and disseminate a list of permitted technologies and applications;
2. Inform employees of which applications are blacklisted and require reading of the disclaimer;
3. Implement monitoring tools that allow the detection and alert of blacklisted applications;
4. Integrate device manager events into existing SIEM;
5. Require formal authorization for requested exceptions when:
    a. An employee requires it to perform its daily activities;
    b. It is a required dependency for other vendors’ software.

Evidences

1. List of authorized software;
2. List of blacklisted software;
3. Disclaimer for reasonable IT resource usage;
4. Support documents for SIEM.

N.R. COBIT 5 APO07.06, APO10.05;

ISO/IEC 27001:2013 A.14.2.7, A.15.2.1;

NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4.

DE.MC-6 - External service provider activity is monitored to detect potential cybersecurity events

Description

Services provided by contractors should be monitored to detect unauthorized accesses on networks and information systems.

Technical Implementation

1 SIEM;

2 Intrusion detection and prevention system (IDS/IPS).

Process Implementation

The organization should:

1 Identify on the supplier management policy:
   a. The monitoring activities of the services provided to the organization;
   a. Security requirements, roles and responsibilities for suppliers;

2 Require that service providers follow the established security policies;

3 Ensure external contractors respect the information confidentiality of the data they access when performing their activities;

4 Require suppliers to notify when an external contractor that worked for the organization leaves or retires;

5 Monitor security events caused by external contractors. Create and investigate security incidents derived from those events.

Evidences

1 Support document for supplier management policy;

2 Reports of past security incidents caused by external service providers.

N.R. CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16;

COBIT 5 DSS05.02, DSS05.05;

ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1;

NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4.

DE.MC-7 - Monitoring for unauthorized personnel, connections, devices and software is performed

Description

The organization should monitor network and information system accesses by employees, devices, equipments and processes that might not have the proper authorizations.

Technical Implementation

1. SIEM;
2. Intrusion detection and prevention system (IDS/IPS).

Process Implementation

The organization should:

1. Monitor accesses to networks and information systems and correlate them with the list of authorized accesses;
2. Collect events from ad-hoc locations to attempt detection of anomalous accesses;
3. Report detected unauthorized accesses;
4. Create, investigate and resolve security incidents that derive from unauthorized accesses.

Evidences

1. Records of access events to networks and information systems;
2. Records of correlation of unauthorized access events;
3. Incident reports of unauthorized accesses.

N.R. CIS CSC 4, 20;

COBIT 5 BAI03.10, DSS05.01;

ISO/IEC 27001:2013 A.12.6.1;

NIST SP 800-53 Rev. 4 RA-5.

DE.MC-8 - Vulnerability scans are performed

Description

The organization should execute the defined vulnerability management process by performing regular vulnerability scans, both automatically and on demand.

Technical Implementation

1 Vulnerability scanning tools.

Process Implementation

The organization should:

1 Define an execution plan for vulnerability scans;

2 Identify security flaws and report them[1], listing:
  a. Platforms, versions and misconfigurations;
  b. Vulnerability impacts;
  c. Vulnerability descriptions;
  d. Correction procedures;
  e. Validation tests for rebuting false positives;

3 Act on vulnerability reports, implementing corrections or mitigations for the identified vulnerabilities.

Evidences

1 Support document for vulnerability management process;

2 Reports from past vulnerability scans;

3 Records from past corrections or mitigations.

4.5.3 DE.PD Detection Processes

N.R. CIS CSC 19;

COBIT 5 APO01.02, DSS05.01, DSS06.03;

ISO/IEC 27001:2013 A.6.1.1, A.7.2.2;

DE.PD-1 - Roles and responsibilities for detection are well defined to ensure accountability

Description

The organization should do awareness sessions that focus on giving stakeholders a clear understanding of the security process, as well as their responsibilities and required activities.

Technical Implementation

Not applicable.

Process Implementation

The organization should define, in the SIEM process:

[1] In case that a legal process exists, it must be applied

1 Who are the stakeholders;

2 What roles and responsibilities they have;

3 In which process phase they should intervene;

4 What is the escalate process;

5 Event classification taxonomy;

6 The awareness sessions that should occur.

Evidences

1 Support documents for SIEM;

2 Support documents for incident handling;

3 Records from awareness sessions.

N.R. COBIT 5 DSS06.01, MEA03.03, MEA03.04;

ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3;

NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14.

DE.PD-2 - Detection activities comply with all applicable requirements

Description

The organization should perform internal audits that can measure the effectiveness of the detection services and identify possible non-conformities and the respective improvements.

Technical Implementation

1 SIEM.

Process Implementation

The organization should:

1 Define an annual audit plan;

2 Define the evaluation methodology to measure the efficiency of detection activities;

3 Verify if environments, roles, responsibilities and teams are properly defined;

4 Verify the compliance and performance of detection activities;

5 Define a plan of activities when improvements are identified.

Evidences

1 Audit plan;

2 Audit reports;

3 Improvement suggestions and plan of activities.

N.R. COBIT 5 APO13.02, DSS05.02;

ISO/IEC 27001:2013 A.14.2.8;

NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14.

DE.PD-3 - Detection processes are tested

Description

The organization should test and verify the performance of the detection processes when:

1 A significant system change occurs;

2 A significant new application development is made;

3 A new system is added to the current infrastructure;

4 A new vulnerability type is brought to light.

Technical Implementation

1 SIEM;

Process Implementation

The organization should:

1 Identify the objectives to be achieved with the tests;

2 Define the testing plan;

3 Define and execute the required activities;

4 Formalize the test execution and produce a report of the performed activities;

5 Validate if the results are in line with the expected performance or if improvements are needed;

6 Establish a plan for improvements when needed.

Evidences

1 Test plan records;

2 Improvement plan records.

N.R. CIS CSC 19;

COBIT 5 APO08.04, APO12.06, DSS02.05;

ISO/IEC 27001:2013 A.16.1.2, A.16.1.3;

NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4.

DE.PD-4 - Event detection information is communicated

Description

The organization should define a communication strategy that keeps relevant stakeholders informed about security incidents or serious security events. The strategy should be supported on a communication plan that can be consolidated with other communication plans.

Technical Implementation

1 Incident handling process tool.

Process Implementation

The incident handling process should have a well defined communication plan. The plan should, at least, identify:

1 What to communicate: Content (e.g.: incident description and impacts);

2 What message: Form and format, what type of media will be used, from small texts with images, metaphors, videos;

3 Who should communicate: An individual should be nominated to engage with external organizations and should have autonomy and authority to do so;

4 To whom communicate: Communication recipients;

5 How to communicate: Which channels should be used to efficiently share the message (e.g.: email messages);

6 When to communicate: The communication should be exercised regularly and in normal conditions (e.g.: sharing the information security policy), but can have different frequencies and different modes of engagement depending on the incident context.

Evidences

1 Support documents for incident handling;

2 Records of event communications that originate from security incidents.

N.R. COBIT 5 APO11.06, APO12.06, DSS04.05;

ISO/IEC 27001:2013 A.16.1.6;

NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14.

DE.PD-5 - Detection processes are continuously improved

Description

The organization should learn from past incidents that occur in their networks and information systems by identifying the operational and/or processual measures that can improve the detection capacity for new incidents.

Technical Implementation

Not applicable.

Process Implementation

The organization should define:

1 The review and learning procedure from event detection processes;

2 Improvement activities identified on the detection process tests.

Evidences

1 Improvement plan of detection processes;

2 Records from improvement activities.

SECURITY MEASURES

RESPOND

4.6.1 RS.PR Response planning

N.R. CIS CSC 19;

COBIT 5 APO12.06, BAI01.10;

ISO/IEC 27001:2013 A.16.1.5;

NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8.

RS.PR-1 - Response plan is executed during or after an incident

Description

The organizations should devise an incident response plan to ensure the correct allocation of resources (human, technological). Incident handling resolution should follow a process and have an individual owner for treatment.

When analyzing an incident, evidence chain of custody and integrity must be maintained for any collected artifact.

Technical Implementation

1. Incident handling platform.

Process Implementation

The organization should:

1. Implement an incident handling process that includes containment and eradications;
2. Identify an owner to treat security incidents that will be responsible for coordinating response and contingency activities;
3. Define escalation procedures;
4. Ensure that scope, applicability, rigor and results from incident response activities are consistent and transversal across all the organization and all incidents.

Evidences

1. Support documents for incident response plan;
2. Response records for incident handling.

4.6.2 RS.CO Communications

N.R. CIS CSC 19; COBIT 5 EDM03.02, APO01.02, APO12.03; ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1; NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8.

RS.CO-1 - Personnel know their roles and order of operations when a response is needed

Description

During an incident response, the organization should ensure that all employees are engaged and have knowledge of relevant stakeholder, their roles in the response plan and the activities required to solve the incident.

Technical Implementation

1 Incident handling platform.

Process Implementation

In the incident handling process, the organization should identify:

1 Execution steps for incident response;

2 Stakeholders;

3 Roles and responsibilities of stakeholders.

The organization should perform training sessions to raise awareness of all employees.

Evidences

1 Support document for incident handling;

2 Reports of past awareness training sessions.

N.R. CIS CSC 19; COBIT 5 DSS01.03; ISO/IEC 27001:2013 A.6.1.3, A.16.1.2; NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8.

RS.CO-2 - Incidents are reported according to established criteria

Description

The organization should establish and disseminate the proper channels for incident reporting and the proper information security incident typification to stakeholders.

Technical Implementation

1 Incident response platform.

Process Implementation

The organization should ensure the incident handling plan is well defined and communicated, sharing organization-wide:

1 Proper incident report channels;

2 Security incident categorization;

3 The process to communicate and notify about security incidents, that are ongoing or have been resolved, to authorities, clients, public and third parties, if applicable or needed.

Evidences

1 Support document for the incident handling process;

2 Past security incidents reported by external teams.

N.R. CIS CSC 19;

COBIT 5 DSS03.04;

ISO/IEC 27001:2013 A.16.1.2, Cláusula 7.4, Cláusula 16.1.2;

NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4.

RS.CO-3 - Information is shared according to response plans

Description

The organization should use the proper channels to disseminate information about security incidents to stakeholders. This will help stakeholders detect, contain and resolve similar issues that might occur in their systems.

The communication strategy should be defined in the communication plan. The communication plan can be consolidated with other communication plans.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Identify the communication plan to adopt. The plan can be integrated into other plans;

2 Identify stakeholders, to whom the security incident information should be disseminated;

3 Have secure channels defined for communicating confidential information;

4 Share, in due time, information about security incidents to stakeholders.

Evidences

1 Records identifying stakeholders;

2 Support document for incident handling;

3 Records of past communications to stakeholders.

N.R. CIS CSC 19;

COBIT 5 DSS03.04;

ISO/IEC 27001:2013 Cláusula 7.4;

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.CO-4 - Coordination with stakeholders occurs according to the response plans

Description

The organization should implement a coordination and escalation plan for security incidents, considering the categorization and criticality they have. These plans can be consolidated with other coordination and escalation plans that the organization has.

Technical Implementation

Not applicable.

Process Implementation

In the scope of the incident handling response plan, the organization should identify the following information:

1 Stakeholders and single point of contacts (SPOCs);

2 Communication plan, detailing:
   a. What to communicate: Content (e.g.: incident description and impacts);
   b. What message: Form and format, what type of media will be used, from small texts with images, metaphors, videos;
   c. Who should communicate: An individual should be nominated to engage with external organizations and should have autonomy and authority to do so;
   d. To whom communicate: Communication recipients;
   e. How to communicate: Which channels should be used to efficiently share the message (e.g.: email message);
   f. When to communicate: The communication should be exercised regularly and in normal conditions (e.g.: sharing the information security policy), but can have different frequencies and different modes of engagement depending on the incident context;

3 Definition of responsibilities, scope of work, intervention limits and response times for all intervening parties;

4 Relevant authority contacts.

Evidences

1 Support document for the incident handling plan;

2 Reports from past incident handling responses, that demonstrate the coordination with stakeholders.

N.R. CIS CSC 19;
COBIT 5 BAI08.04;
ISO/IEC 27001:2013 A.6.1.4;
NIST SP 800-53 Rev. 4 SI-5, PM-15.

RS.CO-5 - Voluntary information sharing occurs with external stakeholders

Description

In the response phase of a security incident, the organization should identify the information it will voluntarily share with external stakeholders, to achieve broader cybersecurity situational awareness.

The organization should share information about indicators of compromise to interest groups, so that they can also benefit from this and improve their response times, identifying, detecting, containing and eradicating similar threats in their constituency and influence circle.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Keep a list of relevant stakeholders;

2 Have established secure channels to external stakeholder single point of contacts, for information sharing.

Evidences

1 Records with contacts in regulation bodies and relevant interest groups (technical and legal);

2 Communication plan.

4.6.3 RS.AN Analysis

N.R. CIS CSC 4, 6, 8, 19;

COBIT 5 DSS02.04, DSS02.07;

ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5;

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4.

RS.AN-1 - Notifications from detection systems are investigated

Description

The organization should ensure that events generated by detection systems are investigated, categorized and treated in a consistent way. Serious events should evolve into security incidents.

Technical Implementation

1 SIEM.

Process Implementation

The organization should:

1 Monitor events generated by detection systems;

2 Activate security incident handling protocols when needed;

3 Use appropriate response, considering the incident classification on the response plan.

Evidences

1 Support documents for SIEM;

2 Support documents for incident handling protocols;

3 Reports from past detections that were elevated to security incidents.

N.R. COBIT 5 DSS02.02;

ISO/IEC 27001:2013 A.16.1.4, A.16.1.6;

NIST SP 800-53 Rev. 4 CP-2, IR-4.

RS.AN-2 - The impact of the incident is understood

Description

During the process of incident categorization, the organization should evaluate the incident impact in their assets and to its operations and use the results to define the incident severity.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Define the thresholds for incident impact levels, considering the impact they can cause on the organizations assets and operations;

2 Define the acceptable response times, resolution times, alert levels and priority, considering the incident impact.

Evidences

1 Support document for SIEM;

2 Support document for incident handling: Incident impact taxonomy.

N.R. COBIT 5 APO12.06, DSS03.02, DSS05.07;

ISO/IEC 27001:2013 A.16.1.7;

NIST SP 800-53 Rev. 4 AU-7, IR-4.

RS.AN-3 - Forensics are performed

Description

The organization should provide the necessary resources to enable forensic analysis during the incident handling process.

Technical Implementation

1 SIEM;

2 Raw data collection (disc, memory, network traffic) software.

Process Implementation

The organization should define:

1 Procedures that allow the identification, collection and acquisition of system records and information;

2 Procedures that allow the raw packet capture of discs, memory and networks;

3 Procedures that ensure chain-of-custody integrity for gathered evidences.

Evidences

1 Support document for SIEM;

2 Support document for incident handling.

N.R. CIS CSC 19;
COBIT 5 DSS02.02;
ISO/IEC 27001:2013 A.16.1.4;
NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8.

RS.AN-4 - Incidents are categorized according to the response plans

Description

The organization should ensure that incident categorization is performed, following the rules defined in its security incident handling plan.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Define security incident categorization taxonomy considering the type of incident. For instance, following the national taxonomy for incident[1]:
   a. Malware;
   b. Availability;
   c. Information gathering;
   d. Intrusion attempt;
   e. Intrusion;
   f. Information security;
   g. Fraud;
   h. Abusive content;
   i. Other;

2 Ensure the incident categorization is performed in the incident handling process, following the defined taxonomy;

3 Define what activities to perform considering the type of incident.

Evidences

1 Support document for incident handling: Incident categorization taxonomy;

2 Records from past incident categorization.

[1] Available at the internet site of the Portuguese National Cibersecurity Centre

N.R. CIS CSC 4, 19;

COBIT 5 EDM03.02, DSS05.07;

NIST SP 800-53 Rev. 4 SI-5, PM-15.

RS.AN-5 - Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources

Description

The organization should have a formal process to receive the submission of vulnerabilities from internal or external sources (e.g.: internal tests, vulnerability reports, security researchers).

Each submission should be analyzed, verified and follow the process for security incident handling, unless it is a false positive.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Make available a process to report vulnerabilities, both internally and externally;

2 Provide a process to receive security alerts, recommendations, bulletins from vendors and suppliers, interest groups and others;

3 Consistently evaluate, treat and respond to each submission.

Evidences

1 Support document for vulnerability management process;

2 Records from past subscription to technical interest groups;

3 Records of receiving and treating reported vulnerabilities.

4.6.4 RS.MI Mitigation

N.R. CIS CSC 19;

COBIT 5 APO12.06;

ISO/IEC 27001:2013 A.12.2.1, A.16.1.5;

NIST SP 800-53 Rev. 4 IR-4.

RS.MI-1 - Incidents are contained

Description

The organization should define the processes and procedures to ensure security incidents are effectively contained.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Have the capacity to investigate and decide on what measures to apply, for example:
   a. Malware analysis;
   b. Forensic analysis (gather, investigation and chain-of-custody);
   c. SIEM;

2 Have the capacity to sum up evidences and recommend:
   a. What to do in the short term to contain the incident;
   b. What to do in the long term to resolve it;
   c. What should be segregated from the network;
   d. Which backups can be restored;
   e. Which credentials should be changed or disabled;
   f. Which authentication mechanisms should be improved or strengthened with multiple factors;
   g. Which network connections or sessions should be broken;
   h. Which systems should be updated immediately.

Evidences

1 Support document for incident handling responses;

2 Reports from dealing with past security incidents.

N.R. CIS CSC 4, 19;

COBIT 5 APO12.06;

ISO/IEC 27001:2013 A.12.2.1, A.16.1.5;

NIST SP 800-53 Rev. 4 IR-4.

RS.MI-2 - Incidents are mitigated

Description

The organization should define processes and procedures to ensure security incidents are effectively mitigated.

Technical Implementation

Not applicable.

Process Implementation

The organization should:

1 Contain the incident (block accounts or services and websites, segregate networks or user accounts, suspend internet access, reset passwords, close network

ports, disconnect information systems);

2 Reduce the impact (provision of new servers, graceful degradation services, seek alternative temporary services);

3 Eradicate:
   a. Remove the malware used in the attack;
   b. Apply security patches;
   c. Restore backups when needed;
   d. Force password resets or request second factors for authentication;

4 Document:
   a. What systems were compromised;
   b. Root cause analysis;
   c. Data leaked.

Evidences

1 Support document for incident handling;

2 Records of past incident responses.

N.R. CIS CSC 4;

COBIT 5 APO12.06;

ISO/IEC 27001:2013 A.12.6.1;

NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5.

RS.MI-3 - Newly identified vulnerabilities are mitigated or documented as accepted risks

Description

Newly identified vulnerabilities should be formally evaluated by the organization, considering the scope of activities defined in the vulnerability management process. The organization should identify what treatment to give to these vulnerabilities.

Technical Implementation

Not applicable.

Process Implementation

The organization should evaluate new activities:

1 And remedy them;

2 Or execute the required formal procedures for approval of associated risk, justifying the reasons of whatever decision is made.

Evidences

1 Support document for vulnerability management process;

2 Records from past execution of vulnerability management process;

3 Records of vulnerabilities whose risk has been accepted by management.

4.6.5 RS.ME Improvements

N.R. COBIT 5 BAI01.13;

ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.ME-1 - Response plans incorporate lessons learned

Description

The organization should research past incidents after they are resolved to identify lessons that can be learned from them.

The organization should promote work sessions with the incident handling team and brainstorm what can be learned from that particular incident. These work sessions should analyse and document all that is known about the incident, identifying what worked out well and what needs to be improved in the incident handling process to make the organization and its systems more resilient when dealing with future incidents.

Technical Implementation

Not applicable.

Process Implementation

The organization should implement an improvement plan considering the lesson learned, such as:

1 Which changes can be performed to improve security;

2 What can be done in a different way;

3 What should be done in a better way;

4 Who needs training in a skill;

5 Which weaknesses were exploited;

6 How can we ensure it does not happen again.

Evidences

1 Support document for the incident handling plan;

2 Records of improvement actions that originated from lessons learned.

N.R. COBIT 5 BAI01.13; DSS04.08;

ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RS.ME-2 - Response strategies are updated

Description

Threats and vulnerabilities are evolving daily. To keep the incident handling plan updated and relevant, the organization should improve it constantly, incorporating the best practices known at the time.

The organization itself is a dynamic entity. Assets, employees and asset owners can change and, consequently, incident handling plans should be updated to match internal changes.

Technical Implementation

Not applicable.

Process Implementation

The organization should keep updated:

1 The list of networks and information systems that support critical assets;

2 Tactical responses to specific threats;

3 Contact list with external organizations;

4 Internal contact list.

Evidences

1 Support document for the incident handling plan;

2 Version updates to the incident handling plan.

SECURITY MEASURES

RECOVER

4.7.1 RC.PR Recovery Planning

N.R. CIS CSC 10;

COBIT 5 APO12.06, DSS02.05, DSS03.04;

ISO/IEC 27001:2013 A.16.1.5;

NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8.

RC.PR-1 - Recovery plan is executed during or after a cybersecurity incident

Description

The organization should structure its incident recovery plan to ensure proper allocation of resources (human and technological) for incident resolution.

The information security incident recovery process must ensure the integrity and availability of assets that support critical business activities.

Technical Implementation

1 Backup and restore solution.

Process Implementation

The organization should:

1 Implement an incident recovery process;

2 Ensure that the rigor, scope, applicability and results from recovery activities are consistent and transversal to the whole organization and for all incidents;

3 Evaluate and prioritize the set of incident recovery activities, considering other plans such as business continuity plan.

Evidences

1 Support document for incident handling;

2 Reports from past incident recovery activities.

4.7.2 RC.PR Improvements

N.R. COBIT 5 APO12.06, BAI05.07, DSS04.08;

ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RC.ME-1 - Recovery plans incorporate lessons learnt

Description

The organization should ensure the recovery plans are updated with actions from previous lessons learnt.

Technical Implementation

Not applicable.

Process Implementation

The organization should implement an improvement plan based on lessons learnt, considering:

1. Evaluate effectiveness of existing recovery plans;
2. Identify weaknesses in existing plans;
3. Identify improvement oportunites that can be implemented;
4. Update the plan with the improvement.

Evidences

1. Support document for incident handling;
2. Action plan from lessons learnt evaluation.

N.R. COBIT 5 APO12.06, BAI07.08;

ISO/IEC 27001:2013 A.16.1.6, Cláusula 10;

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8.

RC.ME-2 - Recovery strategies are updated

Description

The organizations are dynamic and there are changes at the asset, human resource and asset owner level. The recovery plans should follow this natural evolution with updates to the single point of contact, assets and priorities.

The organization should ensure its recovery strategies are reviewed and updated.

Technical Implementation

Not applicable.

Process Implementation

The organization should update:

1. The priority list of information systems and networks that support critical assets;
2. Recovery techniques for information systems;
3. Contact list for technical owners;

4 Contact list for business owners.

Evidences

1 Support document for the incident recovery plan;

2 Version updates to the incident recovery plan.

4.7.3 RC.CO Communications

N.R. COBIT 5 EDM03.02;

ISO/IEC 27001:2013 A.6.1.4, Cláusula 7.4.

RC.CO-1 - Public relations are managed

Description

The organization should communicate what is relevant in the cybersecurity context. The information flow should be set by the organization to minimize potential reputation and credibility impacts.

The organization should define a communication strategy based on the communication plan. The plan can and should be consolidated with existing plans.

Technical Implementation

Not applicable.

Process Implementation

The organization should define a communication plan with stakeholders, that identifies:

1 What to communicate: Content (e.g.: incident description and impacts);

2 What message: Form and format, what type of media will be used, from small texts with images, metaphors, videos;

3 Who should communicate: An individual should be nominated to engage with external organizations and should have autonomy and authority to do so;

4 To whom communicate: Communication recipients;

5 How to communicate: Which channels should be used to efficiently share the message (e.g.: email message);

6 When to communicate: The communication should be exercised regularly and in normal conditions (e.g.: sharing the information security policy), but can have different frequencies and different modes of engagement depending on the incident context.

Evidences

1 Comunication plan associated to incident recovery.

N.R. COBIT 5 APO12.06;

ISO/IEC 27001:2013 Cláusula 7.4;

NIST SP 800-53 Rev. 4 CP-2, IR-4.

RC.CO-2 - Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

Description

The organization should ensure that internal and external stakeholders are informed when a security incident is serious enough.

The organization should define a communication strategy based on the defined communication plan, which can and should be consolidated into other existing communication plans.

Technical Implementation

Not applicable.

Process Implementation

The organization should define:

1 Procedure for incident escalation;

2 Which incident typification can prompt the contact with external stakeholders;

3 Which communication plan to enact;

4 Whom to contact.

Evidences

1 Communication plan documented and disseminated to the relevant owners.

Additional Recommendations

5.1 Introduction

Nowadays, almost all organizations have security equipments deployed in their communication networks, such as firewalls, intrusion detection systems, name resolution request filters, protection against email spam or email phishing, persistent threat detection tools and more. These equipments are a first line of defense constituting basic measures for the employee and the organization's networks and information systems security against cyber attacks and unregulated Internet traffic.

Are these technologies alone sufficient to ensure the information security of the organization?

It is not possible to give a concrete answer to this question, as it depends on several evaluation variables that change according to the technology, resources, context and surrounding environment of the organization. In practice, these equipments provide immediate protection against known threats (if properly configured) but may be inefficient with what is still unknown.

According to MITRE[1], the number of CVEs (published vulnerabilities per year) has increased significantly in recent years, as can be seen in the chart below.

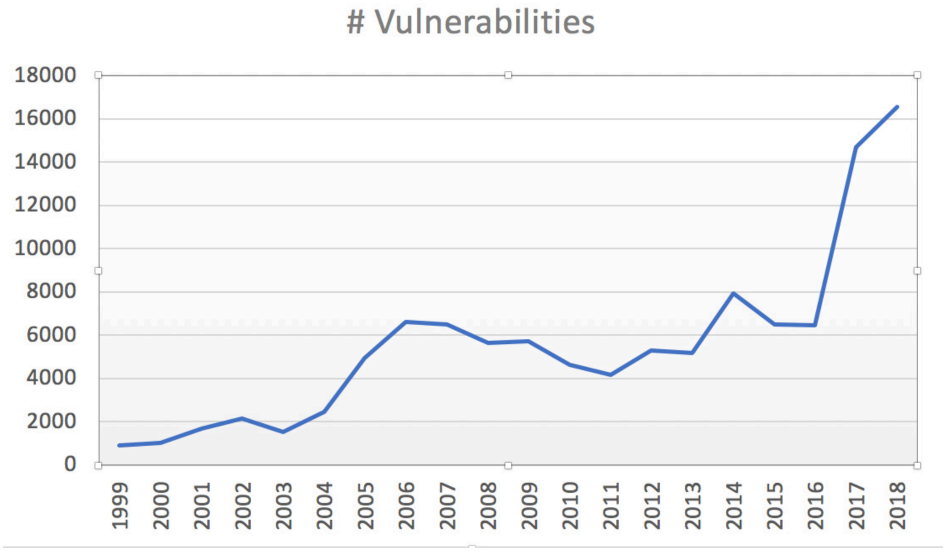

Figure 8 - Number of vulnerabilities published per year

Each of these potential vulnerabilities existing in the organization's networks and information systems could be exploited by a new threat.

Defense perimeters are usually static and are not continuously updated which rises another major challenge for organizations, given the fact that the existing threats from cyberspace are rather dynamic.

In response to these challenges, it is necessary to have a specialized and multidisciplinary team that can serve the organization, continuously updating the protection of its networks and information systems against new cybersecurity threats or even the evolution of old threats.

[1] https://cve.mitre.org/

5.2 The CISO role

CISO, the Chief Information Security Officer, is a role performed in the organization, for which a contractual relationship is established, in order to ensure the information security of that organization.

The CISO should report to top management and, as the impact of this responsibility is potentially crosscutting, must be fully aware of the key processes of the organization in which he works in.

Generally speaking, the CISO should be able to translate the organization's goals into information security requirements and, for this reason, should also be a good communicator.

Among others, the CISO responsibilities include:

- Ensure the implementation and maintenance of the information security strategy;
- Implement holistic and structured information security best practices;
- Research, define and communicate information security requirements;
- Develop and implement information security policies, processes and procedures;
- Have knowledge about the specific legislation and regulation of the organization's activity sector;
- Have knowledge about the laws and regulations referring to information security, namely ISO / IEC 27001 and the General Data Protection Regulation;
- Coordinate efforts regarding personal data protection;
- Define and implement risk assessment and response strategies;
- Monitor and evaluate the implementation of the change management process;
- Monitor and participate in the incident management process;
- Follow security audits and the implementation of improvement measures;
- Foster information security and cybersecurity awareness sessions.

CISO has a pivotal role in NCF-PT analysis and in identifying measures that may be appropriate for implementation in his organization. It should monitor the entire implementation, prioritization and continuous improvement process of activities that ensure that the organization is prepared and adequately resilient in terms of information security and cybersecurity.

5.3 Building a SOC

According to Gartners[1], definition: “A security operations centre (SOC) can be defined both as a team, often operating in shifts around the clock, and a facility dedicated to and organized to prevent, detect, assess and respond to cybersecurity threats and incidents, and to fulfill and assess local regulatory compliance”.

The SOC’s main roles are:

1. Identification, cataloging, categorization and monitoring of networks and information systems, so staff can be aware of which vulnerabilities can become threats to the organization;

2. Proactivity in detecting malicious activity on networks and information systems. The faster the detection and response, the smaller the effects of the threat may become;

3. Manage vulnerabilities to ensure that networks and information systems are properly up-to-date with available security packages, in order to be protected against threats;

4. Update defenses against new threats. The organization's security perimeter should be reviewed frequently and adjusted with the protections deemed necessary;

5. Event and system log management, security and auditing, in order to enable incident response teams to perform forensic analysis when the organization is exposed to incidents or security breaches.

There are several models of SOC ranging from virtual, part-time and non-exclusive resources, to the multifunction model where teams perform not only security tasks but also operation and monitoring tasks for networks and information systems. We then identify the most common types of SOC and their most relevant characteristics:

Virtual SOC

1. No dedicated facility;

2. Part-time team members and without exclusivity;

3. 9x5 operation with a next business day response;

4. Reactive, only activated when a critical alert or incident occurs.

Dedicated SOC

1. Dedicated facilities;

2. Fully in-house dedicated team;

[1] https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity

3 24x7 operation;

4 Reactive and proactive.

Distributed/Co-managed SOC

1 Dedicated facilities;

2 Internal teams with full and partial allocation;

3 24x7 or 9x5 operation, depending on the physical location;

4 Reactive and proactive;

5 Possibility of sharing responsibilities with specialized cyber security partners.

Command SOC

1 Dedicated facilities;

2 Fully in-house dedicated team;

3 9x5 operation;

4 Reactive and proactive;

5 Provides threat intelligence, situational awareness and additional expertise;

6 Rarely directly involved in day-to-day operations.

Multifunction SOC / network operations centre (NOC)

1 Dedicated facility;

2 Fully in-house dedicated team;

3 24x7 operation;

4 Reactive and proactive;

5 It also provides operation and maintenance services for network or information systems. It is a way of cost optimization so that is no need to support two separate teams in a 24x7 operation.

Fusion SOC

1 Dedicated facility;

2 Fully in-house dedicated team;

3 24x7 operation;

4 Reactive and proactive;

5 Integrates the computer incident response team (CIRT) or the security and network devices operation team.

External SOC

1 No dedicated facility;

2 Full-time external team members;

3 24x7 operation;

4 Reactive and proactive;

5 Supervision of activities performed by someone internal to the organization.

For the planning and implementation of the SOC, the CISO or the organization's general information security and cybersecurity officer shall:

1 Carry out a realistic study of the cost/benefit analysis of the different SOC models before starting to build a fully internal SOC;

2 Focus on the alignment of SOC deliverables with the organization's mission, vision, values, strategies and goals;

3 Define the objectives and metrics that must be met;

4 Identify which critical security functions should be internalized;

5 Consider using expert partner services to minimize SOC 24x7 operating costs and/or to meet additional internal resource capacity needs.

5.4 Constitution of the CSIRT

The abbreviation CSIRT stands for *Computer Security Incident Response Team*.

This term is predominantly used in Europe and corresponds to the protected term CERT, registered in the US by the CERT Coordination Centre (CERT/CC) of the Carnegie Mellon University.

A CSIRT team is a team of computer security experts whose main activity is to respond to incidents. It provides the necessary services to manage and help their users to recover from security breaches that may occur.

Having a dedicated computer security team in place helps organizations to reduce impact and prevent severe incidents.

Other possible benefits are as follows:

1 Have centralized coordination for IT security issues within the organization, with a single point of contact;

2 Centralized specialized IT incident management and response;

3 Have available experts to support and help users recover quickly from incidents;

4 Address legal issues and preserve evidence in the event of legal action;

5 Monitor developments in the field of security;

6 Cooperation on computer security within the experts community.

To properly start the process of creating a CSIRT, it is important to have a clear view of the services it may provide to its customers, often referred to as the "user community". It is therefore important to understand the needs of users to provide them with the right services at the right time and with the right quality[1].

As an international reference, IEFT (Internet Engineering Task Force) RFC2350[2] documents the structure of a CSIRT that should be completed and published in order to facilitate the communication of policies, procedures and services to the covered community, or even to other organizations and/or incident response teams.

A more recent definition at a European level is provided by ENISA[3] which classifies the typical services of a CSIRT team in three categories:

Reactive services

1 Alerts and warnings;

2 Incident Handling:
   a. Incident analysis;
   b. Response to local incidents;
   c. Incident response support;
   d. Incident response coordination;

3 Vulnerability handling:

   a. Vulnerability analysis;
   b. Response to vulnerabilities;
   c. Coordination of vulnerability response;

4 Artifact Handling:
   a. Artifact analysis;
   b. Response to artifacts;
   c. Coordination of response to artifacts.

Proactive Services

1 Awareness campaigns;

2 Follow technology trends;

[1] https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-portugese/at_download/fullReport

[2] https://tools.ietf.org/html/rfc2350#appendix-E

[3] https://www.enisa.europa.eu/topics/csirt-cert-services

3 Security evaluations and audits;

4 Configuration and maintenance of security tools, applications and infrastructure;

5 Development of security tools;

6 Intrusion detection services;

7 Security information dissemination.

Security Quality Management Services

1 Risk analysis;

2 Business continuity and post disaster recovery planning;

3 Security consulting;

4 Safety awareness;

5 Training;

6 Product evaluation and certification.

Creating a CSIRT enables organizations to prepare their ability to respond to information security and cybersecurity incidents. It also enables the organization to increase its ability to respond to information security incidents jointly with other stakeholders, bearing in mind that the CSIRT framework emphasizes the importance of sharing information regarding information security incidents throughout the life cycle of the inherent management processes.

Portugal has a National CSIRT[1], Network, composed of public and private sector organizations, which aims to:

- Establish trust between IT security officers in order to create an environment of cooperation and mutual assistance in incident handling and sharing of security best practices;
- Create indicators and national statistical information on security incidents in order to better identify proactive and reactive countermeasures;
- Create the needed tools for the prevention and rapid response in a wide incident scenario;
- Promote a Cybersecurity culture in Portugal.

The establishment of a CSIRT should be tailored to the reality of the organization, taking into account its size, sector of activity, use of information technology and exposure to the cyberspace.

[1] https://www.redecsirt.pt/

In terms of the maturity of the CSIRT teams, there is already the SIM3 (Security Incident Management Maturity Model), which is based on four vectors: organizational, human, tools and processes. This maturity model includes the assessment of 44 different parameters of a team within these four vectors and will allow any team, once established and operating for some time, to perform a self-assessment. This circumstance will enhance the continuous improvement of the team.

Appendix 1 – Table Summary

The following table provides support for the analysis of the reference information supporting the NCF-PT subcategories.

OBJECTIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
IDENTIFY (ID)	Asset Management (ID.GA)	ID.GA-1 – Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.GA-2 – Software platforms and applications within the organization should be inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.GA-3 – Organizational communication and data flows are mapped	CIS CSC 12 COBIT 5 DSS05.02 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.GA-4 – External information systems are catalogued	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.GA-5 – Resources are prioritized based on their classification, criticality, and business value	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
	Business Environment (ID.AO)	ID.AO-1 – The organization’s role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.AO-2 – The organization’s place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
		ID.AO-3 – Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.AO-4 – Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.AO-5 – Resilience requirements to support the delivery of critical services are established for all operating states	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	Governance (ID.GV)	ID.GV-1 – Organizational cybersecurity policy is established and communicated	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4 -1 controls from all security control families
		ID.GV-2 – Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 NIST SP 800-53 Rev. 4 -1 controls from all security control families
	Risk Assessment (ID.AR)	ID.AR-1 – Asset vulnerabilities are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.AR-2 – Cyber threat intelligence is received from information sharing forums and sources	CIS CSC 4 COBIT 5 BAI08.01 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
		ID.AR-3 – Threats, both internal and external, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.AR-4 – Threats, vulnerabilities, likelihoods and impacts are used to determine risk	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
		ID.AR-5 – Risk responses are identified and prioritized	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9
	Risk Management Strategy (ID.GR)	ID.GR-1 – Risk management processes are established and managed	CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 NIST SP 800-53 Rev. 4 PM-9
		ID.GR-2 – Organizational risk tolerance is determined and clearly expressed	COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9
		ID.GR-3 – Organizational risk treatment strategy is determined and clearly expressed	COBIT 5 APO12.02 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	ID.GL – Supply Chain Risk Management	ID.GL-1 – Cyber supply chain risk management processes are identified, established, assessed, managed and agreed to by organizational stakeholders	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
		ID.GL-2 – Cyber supply chain risks are evaluated	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.GL-3 – Supply chain contracts respect the approved management plan	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
		ID.GL-4 – Suppliers and third-party partners are routinely assessed	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.GL-5 – Response and recovery planning and testing are conducted with suppliers and third-party providers	CIS CSC 19, 20 COBIT 5 DSS04.04 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
PROTECT (PR)	PR.GA – Identity Management, Authentication and Access Control	PR.GA-1 – Identities and credentials are issued, managed, verified, revoked and audited	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.GA-2 – Physical access to assets is managed and protected	COBIT 5 DSS01.04, DSS05.05 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.GA-3 – Remote access is managed	CIS CSC 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.GA-4 – Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.GA-5 – Network integrity is protected	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.GA-6 – Identities are proofed and bound to credentials and asserted in interactions	CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.GA-7 – Users, devices and other assets are authenticated commensurate with the risk of the transaction	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	PR.FC – Awareness and Training	PR.FC-1 – All users are informed and trained	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.FC-2 – Privileged users understand their roles and responsibilities	CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.FC-3 – Third-party stakeholders understand their roles and responsibilities	CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04, APO10.05 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
		PR.FC-4 – Senior executives understand their roles and responsibilities	CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	PR.SD – Data Security	PR.SD-1 – Data-at-rest is protected	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
		PR.SD-2 – Data-in-transit is protected	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 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 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
		PR.SD-3 – Assets are formally managed throughout removal, transfers and disposition	CIS CSC 1 COBIT 5 BAI09.03 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.SD-4 – Adequate capacity to ensure availability is maintained	CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.SD-5 –Protections against data leaks are implemented	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02 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.10.1.1, A.11.1.4,A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.SD-6 – Integrity checking mechanisms are used to verify software, firmware, and information integrity	CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 NIST SP 800-53 Rev. 4 SC-16, SI-7
		PR.SD-7 – The development and testing environment(s) are separate from the production environment	CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
		PR.SD-8 – Integrity checking mechanisms are used to verify hardware integrity	COBIT 5 BAI03.05 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
		PR.PI-11 – Cybersecurity is included in human resources practices	CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.PI-12 – A vulnerability management plan is developed and implemented	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	PR.MA – Maintenance	PR.MA-1 – Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6
		PR.MA-2 – Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access	CIS CSC 3, 5 COBIT 5 DSS05.04 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
	PR.TP – Protective Technology	PR.TP-1 – Audit/log records are determined, documented, implemented and reviewed in accordance with the policies	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 NIST SP 800-53 Rev. 4 AU Family
		PR.TP-2 – Removable media is protected and its use restricted, according to policy	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.TP-3 – The principle of least functionality is incorporated	CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISO/IEC 27001:2013 A.9.1.2 NIST SP 800-53 Rev. 4 AC-3, CM-7
		PR.TP-4 – Communications and control networks are protected	CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.TP-5 – Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
DETECT (DE)	DE.AE – Anomalies and Events	DE.AE-1 – A baseline of network operations and expected data flows for users and systems is established and managed	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
		DE.AE-2 – Detected events are analyzed to understand attack targets and methods	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3 – Event data are collected and correlated from multiple sources and sensors	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5 BAI08.02 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4 – The impact of events is determined	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4
		DE.AE-5 – Incident alert thresholds are established	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	DE.MC – Monitoring	DE.MC-1 – The network is monitored to detect potential cybersecurity events	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.MC-2 – The physical environment is monitored to detect potential cybersecurity events	COBIT 5 DSS01.04, DSS01.05 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.MC-3 – Personnel activity is monitored to detect potential cybersecurity events	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.MC-4 – Malicious code should be detected	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
		DE.MC-5 – Unauthorized mobile applications are detected	CIS CSC 7, 8 COBIT 5 DSS05.01 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
		DE.MC-6 – External service provider activity is monitored to detect potential cybersecurity events	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4
		DE.MC-7 – Monitoring for unauthorized personnel, connections, devices and software is performed	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.MC-8 – Vulnerability scans are performed	CIS CSC 4, 20 COBIT 5 BAI03.10, DSS05.01 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	DE.PD – Detection Processes	DE.PD-1 – Roles and responsibilities for detection are well defined to ensure accountability	CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.PD-2 – Detection activities comply with all applicable requirements	COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.PD-3 – Detection processes are tested	COBIT 5 APO13.02, DSS05.02 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.PD-4 – Event detection Information is communicated	CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.PD-5 – Detection processes are continuously improved	COBIT 5 APO11.06, APO12.06, DSS04.05 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	RS.PR – Response planning	RS.PR-1 – Response plan is executed during or after an incident	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
	RS.CO – Communications	RS.CO-1 – Personnel know their roles and order of operations when a response is needed	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2 – Incidents are reported consistent with established criteria	CIS CSC 19 COBIT 5 DSS01.03 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3 – Information is shared consistent with response plans	CIS CSC 19 COBIT 5 DSS03.04 ISO/IEC 27001:2013 A.16.1.2, Clause 7.4, Clause 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4 – Coordination with stakeholders occurs consistent with response plans	CIS CSC 19 COBIT 5 DSS03.04 ISO/IEC 27001:2013 Clause 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5 – Voluntary information sharing occurs with external stakeholders	CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
	RS.AN – Analysis	RS.AN-1 – Notifications from detection systems are investigated	CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2 – The impact of the incident is understood	COBIT 5 DSS02.02 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3 – Forensics are performed	COBIT 5 APO12.06, DSS03.02, DSS05.07 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4 – Incidents are categorized consistent with response plans	CIS CSC 19 COBIT 5 DSS02.02 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8
		RS.AN-5 – Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources	CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15
	RS.MI – Mitigation	RS.MI-1 – Incidents are contained	CIS CSC 19 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2 – Incidents are mitigated	CIS CSC 4, 19 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3 – Newly identified vulnerabilities are mitigated or documented as accepted risks	CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	RS.ME – Improvements	RS.ME-1 – Recovery plans incorporate lessons learned	COBIT 5 BAI01.13 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.ME-2 – Response strategies are updated	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

OBJETIVE	CATEGORY	SUBCATEGORY	BACKGROUND INFORMATION
RECOVER (RC)	RC.PR – Recovery Planning	RC.PR-1 – Recovery plan is executed during or after a cybersecurity incident	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	RC.ME – Improvements	RC.ME-1 – Recovery plans incorporate lessons learned	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.ME-2 – Recovery strategies are updated	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Clause 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	RC.CO – Communications	RC.CO-1 – Public relations are managed	COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Clause 7.4
		RC.CO-2 – Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Clause 7.4

Table 11 – Table Summary

www.cncs.gov.pt
cncs@cncs.gov.pt

Rua da Junqueira 69,
1300-342 Lisboa
+351 210 497 400

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL