DG DIGIT
Unit S1 – IT Security Policy

Detailed Catalogues

IT Security Risk Management Methodology v1.2

Date: 11/08/2020
Doc. Version : v1.2 r11

Document Control Information

Settings	Value
Document Title:	IT Security Risk Management Methodology v1.2 – Detailed Catalogues
Project Title:	IT Security Risk Management Methodology v1.2
Programme Name:	IT Security Risk Management Programme
Document Author:	Rodolfo MUNOZ ORTEGA Thomas HERLEA Joël HUBIN
Programme Owner (PgO):	Grzegorz MINCZAKIEWICZ
Programme Business Manager (PgBM):	Spyros SARIGIANNIDIS
Programme Manager (PgM):	Liliana MUSETAN
Doc. Version:	v1.2 r11
Sensitivity:	Internal
Date:	11/08/2020

Document Approver(s) and Reviewer(s):

NOTE: All Approvers are required. Records of each approver must be maintained. All Reviewers in the list are considered required unless explicitly listed as Optional.

Name	Role	Action	Date
Grzegorz MINCZAKIEWICZ	PgO	*Approve*	06/08/2020

Document history:

The Document Author is authorised to make the following types of changes to the document without requiring that the document be re-approved:

- Editorial, formatting, and spelling
- Clarification

To request a change to this document, contact the Document Author or Owner.
Changes to this document are summarised in the following table in reverse chronological order (latest version first).

Revision	Date	Created by	Description (*of Changes*)
10	30/07/2020	JH	Styles and cleaning
11	11/08/2020	LM	Cross-references, foot-notes, doc location

Configuration Management: Document Location

The latest version of this controlled document is stored in:

https://webgate.ec.europa.eu/fpfis/wikis/display/ITSRM2/The+ITSRM+Methodology

TABLE OF CONTENTS

1 INTRODUCTION

As part of the IT Security Risk Management Programme at the European Commission, together with with the recommended IT Security Risk Management (ITSRM) Methodology, DIGIT publishes a range of tools, catalogues and standards to help evaluate and select measures that will effectively address the risk, to complement the efforts of the organisation for the "*protection of the information systems as an integral part of the Functioning of the Commission from IT security incidents that can have a serious impact on the Commission's operations as well as on third parties, including individuals, businesses and Member States*" ([CD46/2017] Recital, point (1)).

The IT Security Risk Management - Detailed Catalogues of elements is part of the knowledge bases for the implementation of the ITSRM Methodology.

The Threats Catalogue from Chapter 2 is a compendium of selected threats from well-known sources like MAGERIT v.3[1], EBIOS[2], OWASP[3], ENISA[4] and CSA[5], detailed in ANNEX A: REFERENCES AND RELATED DOCUMENTS.

The Security Measures Catalogue from Chapter 3 is based on a widely accepted catalogue of security measures: NIST SP-800-53[6]. The ITSRM Methodology only groups the security measures from NIST catalogue into classes which make it clearer what needs to be implemented in order to achieve a risk reduction.

[1] MAGERIT v.3 - Methodology for Information Systems Risk Analysis and Management https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

[2] EBIOS - Expression of Needs and Identification of Security Objectives

[3] OWASP - Open Web Application Security Project

[4] ENISA - https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

[5] CSA - Cloud Security Alliance - https://cloudsecurityalliance.org/

[6] NIST SP 800-53 is shorthand for the National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organization https://nvd.nist.gov/800-53

2 THREATS CATALOGUE

The following is a catalogue of possible threats to the assets in an information system. Each threat is shown in a table as follows:

[code] Short description		
Type of assets that may be affected by this threat	Dimensions [of security] that may be damaged by this threat	Origin: the threat could be accidental (environment) or deliberate (human interaction)
Longer description of the threat		
Source catalogue for the threat		

2.1 [N] Natural

2.1.1 [N.1] Fire

Hardware Locations	[A] Availability	Accidental
Accidental: Possibility that the fire destroys system resources. Concentration of flammable or explosive materials in a confined environment, catching fire through an external event or internal accident.		
MAGERIT v3- Libro 2: Catalogo de elementos - N.1 Fuego EBIOS v2 – Section 4: Tools for assessing ISS risks – 01 Fire		

2.1.2 [N.2] Water

Hardware Locations	[A] Availability	Accidental
Accidental: Possibility that the water destroys system resources. Flood due to a leak or burst pipe.		
MAGERIT v3- Libro 2: Catalogo de elementos - N.2 Daños por agua EBIOS v2 – Section 4: Tools for assessing ISS risks – 02 Water Damage		

2.1.3 [N.*] Other natural disasters

Hardware Locations	[A] Availability	Accidental
Accidental: Other incidents that occur without human involvement: lightning, electric storm, earthquake, cyclones, avalanche, landslide, etc. External event or damage linked to the natural environment close to the assets and capable of causing them very serious physical damage. This excludes specific disasters such as fires (see [N.1]) and floods (see [N.2]). This excludes personnel for whom there is a specific threat [E.28] to cover involuntary non-availability of personnel without going into its causes.		
MAGERIT v3- Libro 2: Catalogo de elementos - N.* Desastres naturales EBIOS v2 – Section 4: Tools for assessing ISS risks – 04 Major incident EBIOS v2 – Section 4: Tools for assessing ISS risks – 06 Climatic Phenomenon EBIOS v2 – Section 4: Tools for assessing ISS risks – 07 Seismic Phenomenon EBIOS v2 – Section 4: Tools for assessing ISS risks – 08 Volcanic Phenomenon EBIOS v2 – Section 4: Tools for assessing ISS risks – 09 Meteorological Phenomenon		

2.2 [I] Industrial

2.2.1 [I.1] Fire

Hardware Locations	[A] Availability	Accidental / Deliberate
Accidental: Possibility that the fire destroys system resources. Deliberate: Terrorists or vandals gaining access to property in order to set light to flammable or explosive materials directly or indirectly (incendiary bombs, tampering with ventilation devices, etc.).		
MAGERIT v3- Libro 2: Catalogo de elementos - I.1 Fuego EBIOS v2 – Section 4: Tools for assessing ISS risks – 01 Fire		

2.2.2 [I.2] Water

Hardware Locations	[A] Availability	Accidental / Deliberate
Accidental: Escapes, leaks, floods: possibility that the water destroys the system's resources. Deliberate: Terrorists or vandals gaining access to the property to cause flooding in the rooms.		
MAGERIT v3- Libro 2: Catalogo de elementos - I.2 Daños por agua EBIOS v2 – Section 4: Tools for assessing ISS risks – 02 Water Damage		

2.2.3 [I.*] Other natural disasters

Hardware Locations	[A] Availability	Accidental / Deliberate
Accidental: Other disasters due to human activity, for example: explosions collapses chemical pollution electrical overloads electrical fluctuations traffic accidents This excludes specific threats such as fire (see [I.1]) and flood (see [I.2]). This excludes personnel for whom there is a specific threat [E.28], to cover involuntary non-availability of personnel without going into its causes. Deliberate: External event or damage linked to an act of vandalism or terrorism close to the assets capable of causing them very serious physical damage.		
MAGERIT v3- Libro 2: Catalogo de elementos - I.* Desastres Industriales EBIOS v2 – Section 4: Tools for assessing ISS risks – 04 Major incident		

2.2.4 [I.3] Environmental pollution

Hardware Locations	[A] Availability	Accidental / Deliberate
Accidental: Presence of dust, vapours, corrosive or toxic gases in the ambient air. Deliberate: Deliberate pollution of the ambient air by tampering with air-conditioning devices or placing a source of pollution in the rooms.		
MAGERIT v3- Libro 2: Catalogo de elementos - I.3 Contaminacion Mecanica EBIOS v2 – Section 4: Tools for assessing ISS risks – 03 Pollution		

2.2.5 [I.4] Electromagnetic pollution

Hardware Locations	[A] Availability	Accidental / Deliberate

Accidental:
Radio interference, magnetic fields, ultraviolet light, etc. Thermal effect caused by a damage or exceptional weather conditions. Damage causing an exceptional electromagnetic effect.
Deliberate:
Device causing a thermal effect resulting in malfunction or destruction of equipment. Person using stray radiation to jam or saturate communications or disturb the operation of an appliance. Electromagnetic pulses from nuclear sources.

MAGERIT v3- Libro 2: Catalogo de elementos - I.4 Contaminacion electromagnetica
EBIOS v2 – Section 4: Tools for assessing ISS risks – 14 Electromagnetic radiation
EBIOS v2 – Section 4: Tools for assessing ISS risks – 15 Thermal radiation
EBIOS v2 – Section 4: Tools for assessing ISS risks – 16 Electromagnetic pulses

2.2.6 [I.5] Hardware or software failure

Hardware Software	[A] Availability	Accidental / Deliberate

Accidental:
Failures in the equipment and/or programs. May be due to a defect in origin or may have arisen during the operation of the system.
In specific-purpose systems, it is sometimes difficult to know whether the failure is of physical or logical origin, but this difference is not usually relevant in terms of consequences.
Deliberate:
Deliberate logical or physical attack causing an equipment item to malfunction.

MAGERIT v3- Libro 2: Catalogo de elementos - I.5 Avería de origen físico o lógico
EBIOS v2 – Section 4: Tools for assessing ISS risks – 28 Equipment failure
EBIOS v2 – Section 4: Tools for assessing ISS risks – 29 Equipment malfunction

2.2.7 [I.6] Power interruption

Hardware	[A] Availability	Accidental / Deliberate

Accidental:
Failure, shutdown or incorrect sizing of the power supply to the assets arising either from the supplier's service or from the internal distribution system
Deliberate:
Sabotage or disturbance of the electrical installation by someone gaining access to the equipment (head-end, low voltage transformer, inverter, etc.)

MAGERIT v3- Libro 2: Catalogo de elementos - I.6 Corte del suministro eléctrico
EBIOS v2 – Section 4: Tools for assessing ISS risks – 12 Loss of power supply

2.2.8 [I.7] Unsuitable temperature and / or humidity conditions

Hardware	[A] Availability	Accidental / Deliberate

Deficiencies in the air conditioning of the premises that exceed the working limits for the equipment: excess heat, excess cold excess humidity, etc.
Accidental:
Failure, shutdown or inadequacy of the air-conditioning service may cause assets requiring cooling or ventilation to shut down, malfunction or fail completely.
Deliberate:
A person can sabotage the equipment used to operate the air-conditioning system (cut off the water or power supply, destroy the system, etc.).

MAGERIT v3- Libro 2: Catalogo de elementos - I.7 Condiciones inadecuadas de temperatura o humedad
EBIOS v2 – Section 4: Tools for assessing ISS risks – 11 Failure of air-conditioning

2.2.9 [I.8] Communications services failure

IT Services	[A] Availability	Accidental / Deliberate

A cut in the capability to transmit data from one place to another. This is typically due to the physical destruction of the physical transport media or to detention in the switching centres, due to either destruction, detention or simple lack of capacity to handle the current traffic.

Accidental:

Disturbance, shutdown or incorrect sizing of telecommunications services (telephone, Internet access, Internet network).

Deliberate:

Sabotage or disturbance of the Telecom installation by someone gaining access to the telecommunications equipment (head-end, PABX, distribution frame, external cables, etc.)

MAGERIT v3- Libro 2: Catalogo de elementos - I.8 Fallo de servicios de comunicaciones

EBIOS v2 – Section 4: Tools for assessing ISS risks – 13 Failure of telecommunication equipment

2.2.10 [I.9] Interruption of other services or essential supplies

IT services Location	[A] Availability	Accidental / Deliberate

Other services or resources on which the operation of the equipment depends, for example, printer paper, toner, coolant, etc.

Accidental:

Incorrect sizing of supplies (printer paper, toner, coolant, etc.).

Deliberate:

Sabotage by someone gaining access to the facilities.

MAGERIT v3- Libro 2: Catalogo de elementos - I.9 Interrupción de otros servicios y suministros esenciales

2.2.11 [I.10] Media degradation

Hardware	[A] Availability	Accidental / Deliberate

Accidental:

A logical or physical event causing an equipment item to malfunction or as the result of the passing of time.

Deliberate:

Deliberate event to provoke an equipment item to fail or malfunction.

MAGERIT v3- Libro 2: Catalogo de elementos - I.10 Degradación de los soportes de almacenamiento de la información

EBIOS v2 – Section 4: Tools for assessing ISS risks – 28 Equipment failure

EBIOS v2 – Section 4: Tools for assessing ISS risks – 29 Equipment malfunction

2.2.12 [I.11] Electromagnetic emanations

Hardware Location	[C] Confidentiality	Deliberate

The fact of making internal data available to third parties by radio. It is a threat in which the issuer is the passive victim of the attack. Almost all electrical devices emit radiation to the exterior that can be intercepted by other equipment (radio receivers) causing a leak of information. This threat is frequently but inaccurately called, a TEMPEST attack ("Transient Electromagnetic Pulse Standard"). Although abusing the original meaning, it is frequent to hear of equipment described as having "TEMPEST protection", meaning that it is designed not to emit electromagnetically anything of interest in case somebody receives it. This threat does not include emissions for the needs of communication media: wireless networks, microwave links, etc. that may be threatened by interception.

Deliberate:

Interfering signals from an electromagnetic source emitted by the equipment (by conduction on the electrical power supply cables or earth wires or by radiation in free space).

Capture of these signals depends on the distance to the targeted equipment or the possibility of connecting to cables or any other conductor passing close to the equipment (coupling phenomenon).

MAGERIT v3- Libro 2: Catalogo de elementos - I.11 Emanaciones electromagnéticas

EBIOS v2 – Section 4: Tools for assessing ISS risks – 17 Interception of compromising interfaces signals

2.3 [E] Errors and unintentional failures

2.3.1 [E.1] User errors

Hardware Software IT Services	[C] Confidentiality [I] Integrity [A] Availability	Accidental
Accidental: Mistakes by persons when using the services, data, etc. A person commits an operating error, input error or utilisation error on hardware or software.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.1 Errores de los usuarios EBIOS v2 – Section 4: Tools for assessing ISS risks – 38 Errors in use		

2.3.2 [E.2] System / Security administrators errors

Hardware Software IT Services	[C] Confidentiality [I] Integrity [A] Availability	Accidental
Accidental: Mistakes by persons with responsibilities for installation and operation of the systems / system's security. A System / Security Administrator commits an operating error, input error or utilisation error on hardware or software.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.2 Errores del administrador EBIOS v2 – Section 4: Tools for assessing ISS risks – 38 Errors in use		

2.3.3 [E.3] Monitoring errors (logs)

Hardware Software IT Services	[I] Integrity	Accidental
Accidental: Unsuitable activity records: lack of records, incomplete records, incorrectly dated records incorrectly attributed records, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.3 Errores de monitorización		

2.3.4 [E.4] Configuration errors

Hardware Software IT Services	[I] Integrity	Accidental
Accidental: The entry of erroneous configuration data. Almost all assets depend on their configuration and this depends on the diligence of the administrator: access privileges, activity flows, activity records, routing, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.4 Errores de configuración		

2.3.5 [E.7] Organisational deficiencies

Personnel	[A] Availability	Accidental
Accidental: When it is not clear who must do exactly what and when, including taking measures on the assets or reporting to the management hierarchy. Uncoordinated actions, errors by omission, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.7 Deficiencias en la organización		

2.3.6 [E.8] Malware diffusion

Software	[C] Confidentiality [I] Integrity [A] Availability	Accidental
Accidental:		

Unintentional propagation of viruses, spy ware, worms, Trojans, logic bombs, etc.
MAGERIT v3- Libro 2: Catalogo de elementos - E.8 Difusión de software dañino

2.3.7 [E.9] Re-routing errors

IT services Software	[C] Confidentiality	Accidental
Accidental: The sending of information via a system or network using, accidentally, an incorrect route that sent the information to a wrong destination. These could be messages among persons, among processes or among both. The case of a routing error involving a delivery error, with the information ending up in the hands of someone unexpected / unknown.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.9 Errores de re-encaminamiento		

2.3.8 [E.10] Sequence errors

IT services Software	[I] Integrity	Accidental
Accidental: The accidental alteration of the order of the messages sent.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.10 Errores de secuencia		

2.3.9 [E.15] Accidental alteration of the information

IT services Software Hardware Location Personnel	[I] Integrity	Accidental
Accidental: The accidental alteration of the information. This threat is only applicable for data in general, since there are specific threats when information is stored on a digital medium		
MAGERIT v3- Libro 2: Catalogo de elementos - E.15 Alteración accidental de la información		

2.3.10 [E.18] Destruction of information

IT services Software Hardware Location Personnel	[A] Availability	Accidental
Accidental: The accidental loss of the information. This threat is only applicable for data in general, since there are specific threats when information is stored on a digital medium		
MAGERIT v3- Libro 2: Catalogo de elementos - E.18 Destrucción de la información		

2.3.11 [E.19] Information leaks

IT services Software Hardware Location Personnel	[C] Confidentiality	Accidental
Accidental: Disclosure due to indiscretion. Verbal indiscretion, electronic media, hard copies, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.19 Fugas de información		

2.3.12 [E.20] Software vulnerabilities

Software	[C] Confidentiality	Accidental

	[I] Integrity [A] Availability	
Accidental: Defects in the code that cause a defective operation without intention on the part of the user but with consequences to the data confidentiality, integrity, availability or to its capacity to operate		
MAGERIT v3- Libro 2: Catalogo de elementos - E.20 Vulnerabilidades de los programas (software)		

2.3.13 [E.21] Defects in software maintenance / updating

Software	[I] Integrity [A] Availability	Accidental
Accidental: Defects in the procedures or controls for updating the code that allow programs with known defects that have been repaired by the manufacturer to continue to be used. Design error, installation error or operating error committed during modification causing incorrect execution.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.21 Errores de mantenimiento / actualización de programas (software) EBIOS v2 – Section 4: Tools for assessing ISS risks – 31 Software malfunction EBIOS v2 – Section 4: Tools for assessing ISS risks – 32 Breach of information system maintainability		

2.3.14 [E.23] Defects in hardware maintenance / updating

Hardware	[A] Availability	Accidental
Accidental: Defects in the procedures or controls for updating equipment that allow its operation under normal circumstances. Lack of expertise in the system making retrofitting and upgrading impossible; for example, inability to correct an operating problem or respond to new needs		
MAGERIT v3- Libro 2: Catalogo de elementos - E.23 Errores de mantenimiento / actualización de programas (hardware) EBIOS v2 – Section 4: Tools for assessing ISS risks – 32 Breach of information system maintainability		

2.3.15 [E.24] System failure due to exhaustion of resources

Hardware IT Services	[A] Availability	Accidental
Accidental: The lack of sufficient resources causes the system failure when the workload is excessive. Overload of storage space (e.g. back-up space, mailbox storage, work area, etc.) for example, saturation of a mailbox when its owner is absent for long periods. Saturation due to overworking the machine (too many requests processed simultaneously). Equipment incorrectly sized (inverters, communication channels, etc.)		
MAGERIT v3- Libro 2: Catalogo de elementos - E.24 Caída del sistema por agotamiento de recursos EBIOS v2 – Section 4: Tools for assessing ISS risks – 30 Saturation of the information system		

2.3.16 [E.25] Equipment loss

Hardware	[C] Confidentiality [A] Availability	Accidental
Accidental: The loss of equipment directly causes the lack of means to provide services, that is, their service's unavailability. All kinds of equipment can be lose, being the loss of equipment and information supports the most usual. In the case of computers that host data, a leak of information is possible. Retrieval of electronic media (hard discs, floppy discs, back-up cartridges, USB keys, ZIP discs, removable hard discs, etc.) or paper copies (lists, incomplete print-outs, messages, etc.) intended for recycling and containing retrievable information.		
MAGERIT v3- Libro 2: Catalogo de elementos - E.25 Perdida de equipos EBIOS v2 – Section 4: Tools for assessing ISS risks – 22 Retrieval of recycled or discarded media		

2.3.17 [E.28] Staff shortage

Personnel	[A] Availability	Accidental
Accidental:		

Accidental absence from the work post: illness disturbances in public order, bacteriological warfare, etc. Absence of qualified or authorised personnel held up for reasons beyond their control.
MAGERIT v3- Libro 2: Catalogo de elementos - E.28 Indisponibilidad del personal EBIOS v2 – Section 4: Tools for assessing ISS risks – 42 Breach of personnel availability

2.4 [A] Wilful attacks

Wilful attacks are deliberate failures caused by persons. The numbering is not consecutive to match the unintentional errors, which are often similar to deliberate attacks, the only difference being the subject's purpose.

2.4.1 [A.3] Manipulation of activity records

Hardware Software IT Services	[I] Integrity	Deliberate
Deliberate: Manipulation of activity records to remove any evidence or traces.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.3 Manipulación de los registros de actividad (log)		

2.4.2 [A.4] Manipulation of the configuration files

Hardware Software IT Services	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: The entry of erroneous configuration data. Almost all assets depend on their configuration and this depends on the diligence of the administrator: access privileges, activity flows, activity records, routing, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.4 Manipulación de la configuración		

2.4.3 [A.5] Masquerading of identity

Software IT Services	[C] Confidentiality [I] Integrity	Deliberate
Deliberate: When attackers manage to appear as authorised users, they enjoy the users' privileges for their own purposes. A person assumes the identity of a different person in order to use his/her access rights to the information system, misinform the recipient, commit a fraud, etc. This threat may be perpetrated by internal personnel, by persons outside the organisation or by persons contracted temporarily		
MAGERIT v3- Libro 2: Catalogo de elementos - A.5 Suplantación de la identidad del usuario EBIOS v2 – Section 4: Tools for assessing ISS risks – 40 Forging of rights		

2.4.4 [A.6] Abuse of access privileges

Software IT Services Location	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: Each user enjoys a level of privileges for a specific purpose. When users abuse their privilege level to carry out tasks that are not their responsibility, there are problems. Someone accesses the system to modify, delete or add operating characteristics or carry out any other unauthorised operation possible to holders of these rights		
MAGERIT v3- Libro 2: Catalogo de elementos - A.6 Abuso de privilegios de acceso EBIOS v2 – Section 4: Tools for assessing ISS risks – 39 Abuse of rights		

2.4.5 [A.7] Misuse

Software IT Services Location	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: The use of system resources for unplanned purposes, typically of personal interest: games, personal searches on the Internet, personal databases, personal programs, storage of personal data, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.7 Uso no previsto		

2.4.6 [A.8] Malware diffusion

Software	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: Intentional propagation of viruses, spy ware, worms, Trojans, logic bombs, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.8 Difusión de software dañino		

2.4.7 [A.9] Re-routing of messages

IT Services Software	[C] Confidentiality	Deliberate
Deliberate: The sending of information via a system or network using, deliberately, an incorrect route that sent the information to a wrong destination. An attacker may force a message to travel through a specific node in the network where it can be intercepted. Particularly notable is the case in which the routing attack causes a fraudulent delivery, with the information reaching the hands of an unauthorised person.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.9 Re-encaminamiento de mensajes		

2.4.8 [A.10] Sequence alteration

IT services Software	[I] Integrity	Deliberate
Deliberate: The alteration of the order of the messages sent. The idea is that the new order changes the meaning of the group of messages, prejudicing the integrity of the affected data Someone gains access to the communication equipment of the information system and corrupts transmission of information (by intercepting, inserting, destroying, etc.) or repeatedly attempts access until successful.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.10 Alteración de secuencia EBIOS v2 – Section 4: Tools for assessing ISS risks – 36 Corruption of data		

2.4.9 [A.11] Unauthorized access

IT services Software Hardware Location	[C] Confidentiality [I] Integrity	Deliberate
Deliberate: The attacker manages to access the system's resources without authorisation for doing so, typically taking advantage of a failure in the identification and authorisation system. A person inside or outside the organisation accesses the information system and uses one of its services to penetrate it, run operations or steal information.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.11 Acceso no autorizado EBIOS v2 – Section 4: Tools for assessing ISS risks – 33 Unauthorized use of equipment		

2.4.10 [A.12] Traffic analysis

IT Services	[C] Confidentiality	Deliberate

Deliberate: Without needing to analyse the contents of communications, the attacker can reach conclusions based on the analysis of the origin, destination, volume and frequency of the exchanges. This is sometimes called "traffic monitoring"		
MAGERIT v3- Libro 2: Catalogo de elementos - A.12 Análisis de trafico		

2.4.11 [A.13] Repudiation (denial of actions)

IT services	[I] Integrity	Deliberate
Deliberate: A person or entity denies being involved in an exchange with a third party or carrying out an operation. The later rejection of actions or undertakings acquired in the past. Repudiation of origin: denial of being the sender or origin of a message or communication. Repudiation of receipt: denial of having received a message or communication. Repudiation of delivery: denial of having received a message for delivery to others.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.13 Repudio EBIOS v2 – Section 4: Tools for assessing ISS risks – 41 Denial of actions		

2.4.12 [A.14] Eavesdropping

IT Services	[C] Confidentiality	Deliberate
Deliberate: Attackers have access to information that is not theirs, without the information itself being altered. Someone connected to communication equipment or media or located inside the transmission coverage boundaries of a communication can use equipment, which may be very expensive, to listen to, save and analyse the information transmitted (voice or data).		
MAGERIT v3- Libro 2: Catalogo de elementos - A.14 Interceptación de información (escucha) EBIOS v2 – Section 4: Tools for assessing ISS risks – 19 Eavesdropping		

2.4.13 [A.15] Deliberate alteration of the information

IT services Software Hardware Location Personnel	[I] Integrity	Deliberate
Deliberate: Intentional alteration of the information to obtain a benefit or cause damage.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.15 Modificación deliberada de la información		

2.4.14 [A.18] Destruction of information

IT services Software Hardware Location Personnel	[A] Availability	Deliberate
Deliberate: The intentional deletion of information, to obtain a benefit or cause damage.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.18 Destrucción de la información		

2.4.15 [A.19] Disclosure of information

IT services Software Location Personnel	[C] Confidentiality	Deliberate

Deliberate: Intentional disclosure of information. Someone knowingly passing on information inside the organisation to others who have no need to know or to the outside (the latter case usually having greater consequences). Someone with access to equipment used to detect the position of an information system user.
MAGERIT v3- Libro 2: Catalogo de elementos - A.19 Divulgación de información EBIOS v2 – Section 4: Tools for assessing ISS risks – 23 Disclosure EBIOS v2 – Section 4: Tools for assessing ISS risks – 27 Position detection

2.4.16 [A.22] Software manipulation

Software	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: The intentional alteration of the operation of a program to obtain an indirect benefit when an authorised person uses it. The attacker introduces a programme or commands in order to modify the behaviour of a programme or add an unauthorised service to an operating system. This threat agent may act on the information system during the design, pre-production, production, operating, transport or maintenance phase.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.22 Manipulación de programas EBIOS v2 – Section 4: Tools for assessing ISS risks – 26 Tampering with software		

2.4.17 [A.23] Hardware manipulation

Hardware	[C] Confidentiality [A] Availability	Deliberate
Deliberate: The intentional alteration of the operation of a program to obtain an indirect benefit when an authorised person uses it. Someone with access to a communication medium or equipment installs an interception or destruction device in it.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.23 Manipulación de los equipos EBIOS v2 – Section 4: Tools for assessing ISS risks – 25 Tampering with hardware		

2.4.18 [A.24] Denial of services

Hardware IT Services	[A] Availability	Deliberate
Deliberate: The lack of sufficient resources causes the system failure when the workload is too high. An attacker simulates an intense demand on resources by setting up continuous bombardment.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.24 Denegación de servicio EBIOS v2 – Section 4: Tools for assessing ISS risks – 30 Saturation of the Information system		

2.4.19 [A.25] Theft

Hardware	[C] Confidentiality [A] Availability	Deliberate
Deliberate: Theft of equipment directly causes a lack of resources to provide the services, that is, non-availability. All types of equipment may be affected by theft, the most common being theft of equipment and of information media. Theft may be carried out by internal personnel, persons outside the organisation or persons contracted temporarily, which sets different degrees of ease for accessing the stolen object and different consequences. Someone inside or outside the organisation accessing digital media or paper documents with the intention of stealing and using the information on them. Someone inside or outside the organisation accessing equipment located on the premises or transported outside, out of greed or for strategic reasons.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.25 Robo		

EBIOS v2 – Section 4: Tools for assessing ISS risks – 20 Theft of media or documents EBIOS v2 – Section 4: Tools for assessing ISS risks – 20 Theft of Equipment

2.4.20 [A.26] Destructive attack

Hardware Location	[A] Availability	Deliberate
Deliberate: Vandalism, terrorism, military action, etc. This threat may be carried out by internal personnel, by persons outside the organisation or by persons contracted temp		
MAGERIT v3- Libro 2: Catalogo de elementos - A.26 Ataque destructivo EBIOS v2 – Section 4: Tools for assessing ISS risks – 05 Destruction of equipment or media		

2.4.21 [A.27] Enemy over-run

Location	[C] Confidentiality [A] Availability	Deliberate
Deliberate: When the premises have been invaded and control is lost over the means of work		
MAGERIT v3- Libro 2: Catalogo de elementos - A.27 Ocupación enemiga		

2.4.22 [A.28] Staff shortage

Personnel	[A] Availability	Deliberate
Deliberate: Deliberate absence from the work post: such as strikes, labour absenteeism, unjustified absences, the blocking of accesses, etc.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.28 Indisponibilidad del personal EBIOS v2 – Section 4: Tools for assessing ISS risks – 42 Breach of personnel availability		

2.4.23 [A.29] Extortion

Personnel	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: Pressure with threats, on people, to oblige them to act in a certain way.		
MAGERIT v3- Libro 2: Catalogo de elementos - A.29 Extorsión		

2.4.24 [A.30] Social engineering

Personnel	[C] Confidentiality [I] Integrity [A] Availability	Deliberate
Deliberate: Taking advantage of the good will of some persons to make them carry out activities of interest to a third party		
MAGERIT v3- Libro 2: Catalogo de elementos - A.30 Ingeniería social (picaresca)		

2.5 [SR] Services risks (cloud services, services provided by 3rd parties)

2.5.1 [SR.1] Lock-in

IT Services	[A] Availability	Accidental
Accidental: Relying strongly on the services of one provider can lead to severe difficulties in changing the provider. Migrating to another provider may even become virtually impossible.		

This potential dependency for service provision on a particular provider, depending on the provider's commitments, may lead to a catastrophic business failure should the provider go bankrupt and the content and application migration path to another provider is too costly (financially or time-wise) or insufficient warning is given (no early warning).
ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R1 Lock-in

2.5.2 [SR.2] Loss of governance

IT Services	[A] Availability	Accidental / Deliberate
The loss of governance and control could have a potentially severe impact on the organization's strategy and therefore on the capacity to meet its mission and goals. The loss of control and governance could lead to the impossibility of complying with the security requirements, a lack of confidentiality, integrity and availability of data, and a deterioration of performance and quality of service, not to mention the introduction of compliance challenges. Accidental: The provider may outsource or sub-contract services to third-parties (unknown providers) which may not offer the same guarantees (such as to provide the service in a lawful way) as issued by the original provider. Or the control of the poriginal provider changes, so the terms and conditions of their services may also change Deliberate: When using external services, the organization necessarily cedes control to the provider on a number of issues, which may affect security. For example, the provider may prohibit port scans, vulnerability assessment and penetration testing. Moreover, there may be conflicts between customer hardening procedures and the environment.		
ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R2 Loss of governance		

2.5.3 [SR.7] Isolation failure

IT Services	[C] Confidentiality [I] Integrity [A] Availability	Accidental / Deliberate
This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure. The impact can be a loss of valuable or sensitive data, reputation damage and service interruption for cloud providers and their clients. Accidental: In shared environments, errors can lead to situations where one tenant has access to another tenant's resources or data Deliberate: Resource sharing also means that malicious activities carried out by one tenant may affect the reputation of another tenant. For example, spamming, port scanning or the serving of malicious content from infrastructure can lead to: a range of IP addresses being blocked, including the attacker and other innocent tenants of an infrastructure; confiscation of resources due to neighbour activities (neighbour subpoenaed), guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks In the case of attacks, an attacker gets access to the resources or data of a specific customer, or even of all customers of the service.		
ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R7 Isolation failure		

2.5.4 [SR.11] Insecure or ineffective deletion of data

IT Services	[C] Confidentiality	Accidental / Deliberate
Deleting data from storage does not in fact mean that the data is permanently removed from the storage or eventual backup media. If disk storage is not encrypted, the data could be accessed at later time by another customer of an outsourcing partner / provider.		

Accidental:
Resources from a provider (physical hardware, media, etc.) are relocated to other customer and data may be available for a non-authorized user. As example, with cloud providers, where scaling up or down resources; in this context, the probability of a data exposure due to ineffective deletion is considered higher than in a classic IT settings.
Deliberate:
If true data wiping is required, special procedures must be followed and this may not be supported by the standard API (or at all). If this is not done properly malicious attacker can gain access to your data, which should already be deleted.

ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R11 Insecure or ineffective deletion of data

2.5.5 [SR.14] Compromise of Service Engine

IT Services	[C] Confidentiality [I] Integrity [A] Availability	Deliberate

The service engine is a fundamental part of a service. A compromise of the service engine will give an attacker access to the data of all customers, resulting in a potential complete loss of data or denial of service.
Deliberate:
Like any other software layer, the service engine code can have vulnerabilities and is prone to attacks or unexpected failure. An attacker can compromise the service engine by hacking it from inside a system or within the runtime environment, the application pools or through its APIs.

ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R14 Compromise of service engine

2.5.6 [SR.19] Subpoena and e-discovery

IT Services	[C] Confidentiality [A] Availability	Accidental

Law enforcement authorities may ask operators of IT infrastructures to provide information pertaining to criminal cases, or information may have to be provided during civil lawsuits. In some cases, storage media or other hardware might be seized as evidence.
Accidental:
In the event of the confiscation of physical hardware as a result of subpoena by law-enforcement agencies or civil suits, the centralisation of storage as well as shared tenancy of physical hardware means many more clients are at risk of the disclosure of their data to unwanted parties

ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R19 Subpoena and e-discovery

2.5.7 [SR.20] Risk from changing of jurisdiction

IT Services	[C] Confidentiality [A] Availability	Accidental

Accidental:
When data is stored or processed in a data centre located in a country other than the customer country, there are numerous ways in which the change in jurisdiction could affect the security of the information.
Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centres are located in high-risk countries, e.g., those lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreements, etc, sites could be raided by local authorities and data or systems subject to enforced disclosure or seizure.
Data might be seized or the operations of a service disrupted due to reasons that do not exist in the Customer's country. In some cases, national security interests of the hosting country might be cited as a reason for seizing data. Additionally, a service provider might be subject to law enforcement or national security actions from the country its business headquarters is based in, not just those from the countries where its data centres are located.

ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R20 Risk from changes of jurisdiction

2.5.8 [SR.21] Data protection risks

IT Services	[C] Confidentiality	Deliberate

Deliberate:

Data protection law is based on the premise that it is always clear where personal data is located, who process it and who is responsible for data processing. Distributed environments from Service Providers appears to fundamentally conflict with this evidence.

Processing data in another country may incur difficulties regarding data protection legislation, or might even be considered unlawful by the responsible Data Protection authority.

ENISA 2012 - Cloud Computing Benefits, risks and recommendations for information security – R21 Data protection risks

2.5.9 [SR.35] User privacy and secondary usage of data

IT services	[C] Confidentiality	Deliberate

Deliberate:

Customers need to ensure with the providers what data can or cannot be used by them for secondary purposes. It includes data that can be mined directly from user data by providers or indirectly based on user behaviour (clicks, incoming outgoing URLs etc.). Many social application providers mine user data for secondary usage e.g. directed advertising.

OWASP – Cloud top 10 Security Risks –R5 User privacy and secondary usage of data

2.5.10 [SR.38] Incidence analysis and forensics support

IT Services	[C] Confidentiality [I] Integrity [A] Availability	Accidental / Deliberate

In the event of a security incident, applications and services hosted at a provider are difficult to investigate as logging may be distributed across multiple hosts and data centres, which could be located in various countries and hence governed by different laws. Also, along with log files, data belonging to multiple customers may be co-located on the same hardware and storage devices and hence a concern for law enforcing agencies for forensic recovery.

Accidental:

Under the current technological scenario (with multy-tenancy, the dynamic nature of the services, the unification of different data formats, etc.), it is difficult the identification, labelling recording and acquiring of data to be used as part of the incident response.

Deliberate:

In case of incident analysis that requires cross-border data access and exchange, the lack of collaboration mechanisms between the law enforcement agencies and the fragmentations in a multitude of national regulations, make the coordination between the law enforcement agencies problematic and the roles and responsibilities of the actors involved in this type of investigations unclear. An attacker could use this unclarity to delay / stop any investigation.

OWASP – Cloud top 10 Security Risks –R8 Incidence analysis and forensic support

2.5.11 [SR.53] Insecure interfaces and APIs

IT Services	[C] Confidentiality [I] Integrity [A] Availability	Deliberate

Service providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with services. Provisioning, management, orchestration and monitoring are all performed with these interfaces. The security and availability of general services is dependent on the security of these interfaces. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties may build on these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, because organizations may be required to relinquish their credentials to third parties in order to enable their agency.

APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack, and adequate controls protecting them from the Internet are the first line of defense and detection. Deliberate: Weak set of interfaces and APIs exposed by organizations to a variety of security issues related to confidentiality, integrity, availability and accountability. Threats like tampering of data, repudiation, information disclosure, elevation of privilege can be abused by attacker.
CSA 2016 – Top Threats to Cloud Computing-Threat 3: Insecure Interfaces and APIs

3 SECURITY MEASURES CATALOGUE

This catalogue is a summarised version of the NIST 800-53 rev.4 catalogue.

Security measures which achieve a reduction of the impact or likelihood of a risk are grouped under Mitigating Measures. Security measures which by themselves do not directly mitigate risks, but only enable one or more mitigating measures to be effective are grouped under Supporting Measures. There also exist security measures of an exceptional type, related to the supporting measures and implemented not at the level of a System, but higher, organisation-wide. These last security measures are grouped under Corporate Measures.

The NIST catalogue establishes three baselines (Low, Moderate and High) for each security measure in terms of implementing the description of the security measure itself and implementing various subsets of "control enhancements". For ITSRM[2] the sophistication levels are 1, 2 and 3 and they are generally mapped to the NIST baselines, with some exceptions.

Sophistication level is only considered achieved if all measures which support it are either declared as "Not required" for that sophistication level or they also achieved that sophistication level or above (marked as "Same as [*higher level*]" in the catalogues below). For example, implementing sophistication level "Medium" of a mitigating measure means implementing at least the "Medium" baseline for that mitigating measure and for each of its supporting and corporate measures.

The description of each sophistication level of each security measure in this catalogue is just a summary. For the full description the practitioner is directed to consult the NIST catalogue itself.

Each security measure is specified through a table with the following template:

X.Y.Z AA-N – Security Measure Code and Title	
"Alternate Name 1", "Alternate Name 2", ...	
Summary indicating what the measure aims to achieve.	
Supporting and Corporate Measures List of... • ... supporting and... • ... corporate measures	
1	• Description of the best practices of this sophistication level, generally corresponding to the provisions from the corresponding "baseline allocation" from NIST SP-800-53 rev.4
2	• Description of the best practices of this sophistication level, generally corresponding to the provisions from the corresponding "baseline allocation" from NIST SP-800-53 rev.4
3	• Description of the best practices of this sophistication level, generally corresponding to the provisions from the corresponding "baseline allocation" from NIST SP-800-53 rev.4
http://link.to.entry/in/NIST/NVD/AA-N	

3.1 Mitigating Measures

3.1.1 AC-3 – Access Enforcement
"Logical Access Control"
Ensure that the system allows only authorized accesses by users to assets.

Supporting and Corporate Measures	
• AC-2 – Account Management • AC-5 – Separation Of Duties • AC-6 – Least Privilege • AC-7 – Unsuccessful Logon Attempts • AC-8 – System Use Notification • AC-9 – Previous Logon (Access) Notification • AC-10 – Concurrent Session Control • AC-11 – Session Lock • AC-12 – Session Termination • AC-14 – Permitted Actions Without Identification Or Authentication • AC-16 – Security Attributes • AC-22 – Publicly Accessible Content • AC-24 – Access Control Decisions • AC-25 – Reference Monitor • IA-1 – Identification And Authentication Policy And Procedures • IA-2 – Identification And Authentication (Organizational Users) • IA-3 – Device Identification And Authentication • IA-4 – Identifier Management • IA-5 – Authenticator Management • IA-6 – Authenticator Feedback • IA-7 – Cryptographic Module Authentication • IA-8 – Identification And Authentication (Non-Organizational Users) • IA-9 – Service Identification And Authentication • IA-10 – Adaptive Identification And Authentication • IA-11 – Re-Authentication	
1	• Have an access policy. • Have the system intercept access attempts by users. • Ensure that up-to-date information necessary to decide whether to allow or block the access is available. • Take the access decisions in an automated way.
2	Same as for “1”, but with additional best practices from the Supporting Measures
3	Same as for “2”, but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/AC-3	

3.1.2 AC-4 – Information Flow Enforcement

Ensure that the system allows only authorized information transfers within the system and between the system and other systems.

Supporting and Corporate Measures	
None	
1	Not used
2	• Enforce information flow restrictions regardless of what users may ultimately have access to the information from the flows. • Block information flows not needed by the business function of the system. • Block "impossible" information flows, e.g. inbound traffic declaring to have an internal origin. • Block information flow between security domains that would violate security policy, e.g. transferring personally identifiable information to a jurisdiction with weaker safeguards for privacy.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AC-4	

3.1.3 AC-17 – Remote Access

"Trustworthy Remote Access"
Ensure that the system allows remote access only under circumstances decided in advance. Access to assets destined for public access (e.g. public web servers) is not considered remote access.

Supporting and Corporate Measures	
	• AC-2 – Account Management • AC-5 – Separation Of Duties • AC-6 – Least Privilege • AC-7 – Unsuccessful Logon Attempts • AC-8 – System Use Notification • AC-9 – Previous Logon (Access) Notification • AC-10 – Concurrent Session Control • AC-11 – Session Lock • AC-12 – Session Termination • AC-14 – Permitted Actions Without Identification Or Authentication • AC-16 – Security Attributes • AC-22 – Publicly Accessible Content • AC-24 – Access Control Decisions • AC-25 – Reference Monitor • IA-1 – Identification And Authentication Policy And Procedures • IA-2 – Identification And Authentication (Organizational Users) • IA-3 – Device Identification And Authentication • IA-4 – Identifier Management • IA-5 – Authenticator Management • IA-6 – Authenticator Feedback • IA-7 – Cryptographic Module Authentication • IA-8 – Identification And Authentication (Non-Organizational Users) • IA-9 – Service Identification And Authentication • IA-10 – Adaptive Identification And Authentication • IA-11 – Re-Authentication
1	• Establish (decide and apply) restrictions both to remote user access (e.g. interactive) and to remote access by processes acting on behalf of users (e.g. batch). • Authorize (decide, document, obtain approval) in advance which remote accesses to allow.

2	Same as for "1", plus:
	• Monitor remote connections.
	• Protect the Confidentiality and Integrity of the information using cryptography. Use a VPN for a connection to protect the confidentiality and integrity of the content, but be aware that:
	  ○ With a VPN the connection does not stop being "remote access".
	  ○ Availability is not enhanced by VPN.
	  ○ The confidentiality of aspects of the access (e.g. timing, origin etc.) may not be protected.
	  ○ It can affect the organization's ability to monitor the content of the connection.
	•
	• Force remote connections to pass through a limited number of access points to enhance the ability to control remote access activity.
	• Restrict the set of users who can invoke privileged commands when connecting remotely and document in the Security Plan the rationale for allowing it for them.

3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/AC-17	

3.1.4 AC-18 – Wireless Access

"Trustworthy Wireless Access"
Ensure that the system allows remote access only under circumstances decided in advance.

Supporting and Corporate Measures

- AC-2 – Account Management
- AC-5 – Separation Of Duties
- AC-6 – Least Privilege
- AC-7 – Unsuccessful Logon Attempts
- AC-8 – System Use Notification
- AC-9 – Previous Logon (Access) Notification
- AC-10 – Concurrent Session Control
- AC-11 – Session Lock
- AC-12 – Session Termination
- AC-14 – Permitted Actions Without Identification Or Authentication
- AC-16 – Security Attributes
- AC-22 – Publicly Accessible Content
- AC-24 – Access Control Decisions
- AC-25 – Reference Monitor
- IA-1 – Identification And Authentication Policy And Procedures
- IA-2 – Identification And Authentication (Organizational Users)
- IA-3 – Device Identification And Authentication
- IA-4 – Identifier Management
- IA-5 – Authenticator Management
- IA-6 – Authenticator Feedback
- IA-7 – Cryptographic Module Authentication
- IA-8 – Identification And Authentication (Non-Organizational Users)
- IA-9 – Service Identification And Authentication
- IA-10 – Adaptive Identification And Authentication
- IA-11 – Re-Authentication

1	• Design the system to cover the following questions:
	  ○ What wireless connections to allow at all, if any? (which endpoints, what usage etc.)
	  ○ Which configuration options must have specific values and what those values are for the allowed wireless access connections.
	  ○ How to properly implement wireless access
	• Authorize (decide, document, obtain approval) in advance which wireless accesses to allow.

2	Same as for "1", plus: • Authenticate users and/or devices prior to granting them wireless access to the system. • Protect the Confidentiality and Integrity of the traffic using cryptography.
3	Same as for "2", plus: • Restrict which users can configure wireless network capabilities. • Reduce the radio signal coverage area such that as little as possible spills outside the perimeter within which wireless access is intentionally provided.

https://nvd.nist.gov/800-53/Rev4/control/AC-18

3.1.5 AC-19 – Access Control For Mobile Devices

Ensure that the system allows access from mobile devices only under circumstances decided in advance.

Supporting and Corporate Measures

- AC-2 – Account Management
- AC-5 – Separation Of Duties
- AC-6 – Least Privilege
- AC-7 – Unsuccessful Logon Attempts
- AC-8 – System Use Notification
- AC-9 – Previous Logon (Access) Notification
- AC-10 – Concurrent Session Control
- AC-11 – Session Lock
- AC-12 – Session Termination
- AC-14 – Permitted Actions Without Identification Or Authentication
- AC-16 – Security Attributes
- AC-22 – Publicly Accessible Content
- AC-24 – Access Control Decisions
- AC-25 – Reference Monitor
- IA-1 – Identification And Authentication Policy And Procedures
- IA-2 – Identification And Authentication (Organizational Users)
- IA-3 – Device Identification And Authentication
- IA-4 – Identifier Management
- IA-5 – Authenticator Management
- IA-6 – Authenticator Feedback
- IA-7 – Cryptographic Module Authentication
- IA-8 – Identification And Authentication (Non-Organizational Users)
- IA-9 – Service Identification And Authentication
- IA-10 – Adaptive Identification And Authentication
- IA-11 – Re-Authentication

1	• Design the system to cover the following questions:
	  ○ What mobile devices access to allow? (by devices from what manufacturers, what models, configurations, for what uses etc.)
	  ○ Which specific configurations to use for the allowed wireless access connections?
	  ○ How to properly implement organization-controlled mobile devices?
	• Authorize (decide, document and obtain approval) in advance which accesses from mobile devices to allow.

2	Same as for "1", plus: • Make full-device encryption or container encryption mandatory. (whichever is more appropriate)
3	Same as for "2", but with additional best practices from the Supporting Measures

https://nvd.nist.gov/800-53/Rev4/control/AC-19

3.1.6 AC-20 – Use Of External Information Systems

Control through terms and conditions the ways in which authorised users can:

- Access this system from external systems.
- Process, store and transmit information of this system using external systems.

This control is not expected for external systems that interact with assets destined for public access (e.g. public web servers).

Supporting and Corporate Measures	
None	

1	• Adapt the restrictions to the trust relationship with the organization controlling the external system.
	• The focus in this control is not on authorizing the users (that is another control), but on their use of external systems to interact with this system.
	• Use the terms and conditions for the use of this system to enforce the user behaviours that can mitigate risk in the identified scenarios. Specify at least:
	  ○ What can be accessed from an external system;
	  ○ The highest allowed security category for the information transferred to an external system.

2	Same as for "1", plus: • Verify the presence on the external systems of the security controls included in the security plan (e.g. through third-party, independent assessments). • Maintain agreements with the organizations controlling the allowed external systems. • Define the circumstances under which organisation-controlled portable storage devices can be connected to external information systems.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AC-20	

3.1.7 AC-21 – Information Sharing

Support authorised users in taking secure decisions to share information with partners.

Supporting and Corporate Measures	
None	
1	Not used
2	• Enable users to determine if an intended recipient of information is authorized to access the information . • Assist users in making information sharing decisions through automated mechanisms or manual processes.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AC-21	

3.1.8 AC-23 – Data Mining Protection

Prevent the extraction of undesired information by unauthorised parties from high volumes of data exported from the system.

Supporting and Corporate Measures None	
1	• Limit the amount of information which can be exported in bulk from the system. • Limit the speed at which information can be exported in bulk. • Notify personnel when information exported and is reaching a high volume.
2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AC-23	

3.1.9 AT-2 – Security Awareness Training

"General Security Skills"	
Ensure that every member of the organisation knows enough about security to understand the need for it and to be vigilant in their day to day work about security dangers.	
Supporting and Corporate Measures • AT-4 – Security Training Records	

1	• Train users when they join the organisation in the general security skills the system needs them to have.
	• Retrain users when this system has changed enough to require it.
	• Reinforce user security skills periodically to prevent their loss. Examples:
	  ○ Posters, stationery with security reminders;
	  ○ Messages from senior officials;
	  ○ Messages generated by the system (e.g. logon screen messages);
	  ○ Awareness events.

2	Same as for "1", plus: • Include in the training content skills needed for recognizing and reporting insider threats.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AT-2	

3.1.10 AT-3 – Role-Based Security Training

"Specialized Security Skills"
Ensure that every member of the organisation has the security skills necessary for his or her specific role in the organisation.

Supporting and Corporate Measures	
• AT-4 – Security Training Records	
1	Not used

2	• Train users when they assume a new role in the special security skills needed by it before authorizing them to perform that role. Example roles: enterprise architects, developers, procurement officials, system/network administrators, personnel performing independent audit/verification/validation activities.
	• Retrain users when their role has changed enough to require it.
	• Reinforce user security skills periodically to prevent their loss. Examples:
	  ○ Posters in the areas frequented by the roles targeted by the posters;
	  ○ Messages from senior officials;
	  ○ Messages generated by the system (e.g. logon screen messages);
	  ○ Awareness events for groups of users with similar roles.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AT-3	

3.1.11 AU-2 – Audit Events

"Audit Trail"	
Ensure that activity on the system leaves a record that allows reliable after-the-fact investigations of security incidents.	
Supporting and Corporate Measures	
• AU-3 – Content Of Audit Records • AU-4 – Audit Storage Capacity • AU-5 – Response To Audit Processing Failures • AU-6 – Audit Review, Analysis, And Reporting • AU-7 – Audit Reduction And Report Generation • AU-8 – Time Stamps • AU-9 – Protection Of Audit Information • AU-11 – Audit Record Retention • AU-12 – Audit Generation • AU-14 – Session Audit • AU-15 – Alternate Audit Capability • AU-16 – Cross-Organizational Auditing	
1	• Determine what types of events the system is capable of logging. • Coordinate with other organisational entities to determine what information they need from the set determined in the first point. • Determine what subset of the event types from the first point to log, which information to log about each type of event and when (how often or triggered by what situation) each type of event will be audited. • Implement the logging of the information decided in the previous point. • Document why the logged information is deemed adequate to support after-the-fact investigations of security incidents.
2	Same as for "1", plus: • Periodically review and update the set of logged information to ensure that it is both necessary and sufficient.
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/AU-2	

3.1.12 AU-10 – Non-Repudiation

Ensure that actors who have carried out specific types of actions cannot falsely deny later that they have carried them out.

Supporting and Corporate Measures

- AU-3 – Content Of Audit Records
- AU-4 – Audit Storage Capacity
- AU-5 – Response To Audit Processing Failures
- AU-6 – Audit Review, Analysis, And Reporting
- AU-7 – Audit Reduction And Report Generation
- AU-8 – Time Stamps
- AU-9 – Protection Of Audit Information
- AU-11 – Audit Record Retention
- AU-12 – Audit Generation
- AU-14 – Session Audit
- AU-15 – Alternate Audit Capability
- AU-16 – Cross-Organizational Auditing

1	Not used
2	Not used

3	• Cover the following types of actions:
	  ○ Execution of programs;
	  ○ Execution of business processes (e.g. indicating agreement or approval or signing a contract);
	  ○ Creation, deletion, modification of information;
	  ○ Transmission, reception of information.
	• Select and employ non-repudiation techniques applicable to each context (e.g. digital signatures, digital message receipts). See the Supporting Measures, too, for more concrete approaches.

https://nvd.nist.gov/800-53/Rev4/control/AU-10

3.1.13 AU-13 – Monitoring For Information Disclosure

Monitor information sharing Internet locations for the appearance of information leaked from the system.

Supporting and Corporate Measures

- AU-3 – Content Of Audit Records
- AU-4 – Audit Storage Capacity
- AU-5 – Response To Audit Processing Failures
- AU-6 – Audit Review, Analysis, And Reporting
- AU-7 – Audit Reduction And Report Generation
- AU-8 – Time Stamps
- AU-9 – Protection Of Audit Information
- AU-11 – Audit Record Retention
- AU-12 – Audit Generation
- AU-14 – Session Audit
- AU-15 – Alternate Audit Capability
- AU-16 – Cross-Organizational Auditing

1	Not used

2	• Determine likely locations where disclosed information from this system may eventually appear (social media, Pastebin, authorities, CERTs). Monitor those locations for the unauthorized publication of information originating from the System.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/AU-13	

3.1.14 CA-2 – Security Assessments

Ensure that the security measures are implemented and operated correctly and produce the desired results.

Supporting and Corporate Measures

- CA-5 – Plan Of Action And Milestones
- CA-6 – Security Authorization
- CA-7 – Continuous Monitoring

1	• Periodically assesses the security controls of the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome and report the assessment result to the predefined individuals or roles in the organisation. • Carry out the assessment in a systematic way, by determining in advance: o the measures to be assessed, o the assessment procedure for each measure, o the report format documenting the assessment results, o the designated recipients of the assessment reports, o the organization of the assessment (environment, team etc.).
2	Same as for "1", plus: • Employ independent assessors for conducting the assessments.
3	Same as for "2", plus: • Rely in the security assessment on information obtained from other security measures or from specialized assessments (for which there exist dedicated specialists), such as: o SI-4 – Information System Monitoring; o RA-5 – Vulnerability Scanning; o malicious user testing; o insider threat assessment; o performance/load testing
https://nvd.nist.gov/800-53/Rev4/control/CA-2	

3.1.15 CA-3 – System Interconnections

Control the security of dedicated, long-term interconnections with other internal or external information systems.

Supporting and Corporate Measures	
None	

1	• Set up Interconnection Security Agreements with the owners of the other systems to authorize the interconnections.
	• Specify in detail the interconnections:
	  ○ interface characteristics;
	  ○ security requirements;
	  ○ the nature of the information communicated.
	• Periodically review and update the Interconnection Security Agreements to ensure that they correspond to the system's needs.

2	Same as for "1", plus:
	• Use a "blacklisting" or a "whitelisting" strategy for restricting the external interconnections:
	  ○ "Blacklisting" works under the principle "allow all connections, except those that are explicitly prohibited" and is considered the weaker of the two strategies.
	  ○ "Whitelisting" works under the principle "deny all connections, except those that are explicitly permitted" and is considered the stronger of the two strategies.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/CA-3	

3.1.16 CA-8 – Penetration Testing

Determine the degree of resistance of the system to adversaries within a set of specified constraints (e.g., time, resources, and/or skills).

Supporting and Corporate Measures	
None	
1	Not used
2	Not used
3	• Get to an agreement between all parties on the rules of engagement (scope, attack tools/techniques/procedures to be used etc.). • Attempt to duplicate the actions of adversaries in carrying out hostile cyber-attacks. • Perform a more in-depth analysis of the security-related weaknesses/deficiencies found.
https://nvd.nist.gov/800-53/Rev4/control/CA-8	

3.1.17 CA-9 – Internal System Connections

Control the security of internal connections between the elements of the CIS (hence "internal").

Supporting and Corporate Measures	
None	

1	• Authorize the allowed internal connections (it is possible to specify then in terms of classes of components, e.g. “printers”, not in terms of individual components).
	• Specify in detail the internal connections:
	  ○ interface characteristics;
	  ○ security requirements;
	  ○ the nature of the information communicated.

2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/CA-9	

3.1.18 CM-2 – Baseline Configuration

Ensure that the configurable parameters of the system take deliberately chosen, approved values.

Supporting and Corporate Measures

- CM-3 – Configuration Change Control
- CM-4 – Security Impact Analysis
- CM-5 – Access Restrictions For Change
- CM-6 – Configuration Settings
- CM-7 – Least Functionality

1	• Agree upon the sets of specifications for the configurable items within the system (called “baseline configuration”) to be used as the basis for future builds, releases, instances and evolutions of the system. Some configurable items:
	  ○ Names of software packages;
	  ○ Version numbers;
	  ○ Configuration settings/parameters;
	  ○ Network topologies;
	  ○ Component placement in the system architecture.
	• Document the baseline configuration.
	• Formally review the baseline configuration.
	• Maintain the baseline configuration by evolving it to reflect the changes in the system.

2	Same as for “1”, plus:
	• Determine the opportunities to review and update the baseline configuration. Possibilities include:
	  ○ With a given frequency;
	  ○ When required by external circumstances;
	  ○ As an internal part of component installation and upgrade.
	• Retain previous versions of the baseline configuration to support rollback if needed.
	• Foresee the eventuality that components of the system are taken to locations with high risk of attack and issue specific components (e.g. lower value, lower capabilities) with specific configurations (e.g. unnecessary features and unnecessary information removed) before departure

3	Same as for "2", plus: • Use automation to ensure accuracy, e.g. letting the build/deployment system take the configuration values it needs directly from an up-to-date repository for the baseline configuration.

https://nvd.nist.gov/800-53/Rev4/control/CM-2

3.1.19 CM-9 – Configuration Management Plan

Have a plan to control the evolution of the configuration of the system.

Supporting and Corporate Measures

None

1	Not used
2	• Describe the roles, responsibilities, processes and procedures involved in configuration management. • Establish a process for identifying configuration items throughout the development lifecycle and placing them under configuration management. • Describe how changes move through different stages during change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. • Describe the review and approval process for proposed configuration changes prior to implementing them. • Protect the confidentiality of the configuration management plan if it ends up containing information that should have restricted circulation.
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/CM-9

3.1.20 CM-10 – Software Usage Restrictions

"Software Licenses Abidance"

Control the use and handling of software covered by contractual agreements or laws.

Supporting and Corporate Measures

None

1	• Use software only in compliance with the contractual agreements (e.g. software licenses) and relevant laws (e.g. copyright law) • Track the use of software covered by quantity licenses. • Prevent the acquisition and distribution of software in noncompliant ways by members of the organization (e.g. control the use of peer-to-peer file sharing).
2	Not used
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/CM-10

3.1.21 CM-11 – User-Installed Software

Control the installation of software on components of the system by non-administrator users.

Supporting and Corporate Measures	
None	

1	• Define a policy for the installation of software on components of the system by non-administrator users:
	  ○ Identify permitted and prohibited actions regarding software installation (e.g. fresh installations – no, updates and patches - yes).
	  ○
	• Employ technical means (e.g. reduced permissions, scans) and procedural means (e.g. examination of the content of storage controlled by the user, disciplinary action in case of noncompliance) for enforcing the policy.
	• Monitor compliance periodically.

2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/CM-11	

3.1.22 CP-2 – Contingency Plan

Plan the response to information system disruption, compromise, or failure.

Supporting and Corporate Measures	
• CP-3 – Contingency Training • CP-4 – Contingency Plan Testing	

1	• Define the contingency plan, addressing:
	  ○ The contingency requirements of essential mission/business functions;[7]
	  ○ How soon and how much to recover of each function;
	  ○ For essential functions: how to maintain them in spite of the contingency;
	  ○ Who does what in case of contingency;
	  ○ How to fully restore all functions eventually, while maintaining security safeguards.
	• Review and approve the plan by the appropriate senior officials.
	• Coordinate contingency planning with incident handling (as the contingency may be caused by such an incident).
	• Publish copies of the plan to the people with roles in the plan (as this may be impossible during the contingency itself).
	• Periodically review and update the Contingency Plan to ensure that it corresponds to the system's needs. Communicate the changes to the people from the previous point.
	• Protect the confidentiality of the contingency plan if it ends up containing information that should have restricted circulation.

2	Same as for "1", plus:
	• Coordinate the Contingency Plan with any related plans that might exist, e.g.:
	  ○ Business Continuity Plan,
	  ○ Disaster Recovery Plan,
	  ○ Continuity of Operations Plan,
	  ○ Crisis Communications Plan,
	  ○ Critical Infrastructure Plan,
	  ○ Cyber Incident Response Plan,
	  ○ Insider Threat Implementation Plan,
	  ○ Occupant Emergency Plan.
	• Ensure the ability to resume essential mission/business functions.
	• Split the system's assets into critical assets (which support the essential functions) and non-essential asets and use this distinction in prioritising and allocating resources: critical assets may receive additional safeguard and countermeasures.

3	Same as for "2", plus: • Plan to ensure the necessary capacity for information processing, telecommunications and environmental support during contingency operations, given that the threats causing the contingency may have degraded the original capacity. • Plan for the resumption of essential, as well as non-essential mission/business functions. • Plan for ensuring the continuity, not only the resumption of essential mission/business functions
https://nvd.nist.gov/800-53/Rev4/control/CP-2	

3.1.23 CP-6 – Alternate Storage Site

"Geographic Storage Redundancy"
Store a copy of the backup information in at least one other, geographically distinct, site from the primary storage site.
Supporting and Corporate Measures
None

[7] The source document leaves it to the practitioners to select which mission/business functions are essential.

1	Not used
2	• Choose an alternate site to take the place of the primary storage site in the event that the primary site is not available. • Ensure sufficient geographical separation from the primary site to not be affected by the same threats that are taken into consideration for the primary site. • Establish the necessary agreements to store information at the alternate site, to retrieve it from there and to protect it with information security safeguards equivalent to those from the primary site while it is stored there. • Prepare to mitigate access problems to the alternate site in the event of area-wide disruption or disaster. • Start using the alternate storage site and keep it up to date with the primary site.

3	Same as for "2", plus:
	• Configure the alternate site to achieve the desired RTO and RPO for the recovery operations:
	  ○ RTO = "Recovery Time Objective" = "how much time is the recovery allowed to take?";
	  ○ RPO = "Recovery Point Objective" = "how outdated is the recovered state allowed to be?"

https://nvd.nist.gov/800-53/Rev4/control/CP-6	

3.1.24 CP-7 – Alternate Processing Site

"Geographic Processing Redundancy"

Maintain information processing capabilities in at least one other, geographically distinct, site from the primary processing site.

Supporting and Corporate Measures

None

1	Not used

2	• Choose an alternate site to take the place of the primary processing site in the event that the primary site is not available within a defined maximum allowable time.
	• Ensure sufficient geographical separation from the primary site to not be affected by the same threats that are taken into consideration for the primary site.
	• Establish the necessary agreements for taking over essential mission/business functions at the alternate site. The agreements must cover, among others:
	  ○ Access to priority treatment as needed for timely activation of the alternate site;
	  ○ Information security safeguards equivalent to those from the primary site.
	• Ensure that the needed equipment and supplies are available at the alternate site or put contracts in place to have them delivered in time for timely activation of the alternate processing site.
	• Prepare to mitigate access problems to the alternate site in the event of area-wide disruption or disaster.

3	Same as for "2", plus: • Prepare the needed equipment and supplies at the alternate site for timely activation (not only have them available). For example, equipment could be unboxed and configured, ready to take over.
https://nvd.nist.gov/800-53/Rev4/control/CP-7	

3.1.25 CP-8 – Telecommunications Services

"Alternate Telecommunication Services", "Telecommunication Services Redundancy"

Ensure the availability of backup telecommunication services (voice and data) in case the primary

telecommunication services become unavailable for too long at either the primary or secondary processing or storage sites.	
Supporting and Corporate Measures None	
1	Not used.
2	• Establish the necessary agreements for backup telecommunication services. E.g. additional ground-based circuits, an alternate telecommunication services provider, a wireless connection as backup for a landline etc. • Consider factors such as availability, quality of service and access (e.g. for landlines). • Secure access to priority treatment if that is needed for restoring communication capabilities in timely fashion. • Target especially the single points of failure, where the failure of the primary provider would impact the mission/business functions.
3	Same as for "2", plus: • Ensure that there is sufficient separation between the alternate provider and the primary one (e.g. minimal amount of shared infrastructure like trunk line, undersea optic cables etc.) to avoid the alternate provider being impacted by the same threat as the primary one. This is not needed if the primary provider has two sufficiently separated services. • Require the provider to have a contingency plan which can be reviewed and for which the provider can present evidence of periodic contingency training and testing.
https://nvd.nist.gov/800-53/Rev4/control/CP-8	

3.1.26 CP-9 – Information System Backup

"Information Redundancy"	
Provide resiliency against data being destroyed by periodically making copies and protecting them better against loss than the "live" data can be protected.	
Supporting and Corporate Measures • CP-10 – Information System Recovery And Reconstitution	

1	• Create backup copies with the frequency required to achieve the recovery time objectives and the recovery point objectives of the system. Back up:
	  ○ User-level data;
	  ○ System-level data;
	  ○ System documentation, including security documentation;
	• Protect the confidentiality, integrity and availability of the backup copies where they are stored.

2	Same as for "1", plus: • Periodically test the backup copies for integrity/reliability (that the information can be recovered from the storage media),
3	Same as for "2", plus: • Test restoration from backup (by sampling) as part of contingency plan testing. • Store the backups of critical information (which includes inventory, configuration and security information) in a separate facility to protect it from limited disasters (e.g. fire). • Transfer all backup information to the alternate storage site electronically or by physical shipment of storage media. The alternate storage site can serve as the "separate facility" from the previous point.
https://nvd.nist.gov/800-53/Rev4/control/CP-9	

3.1.27 CP-11 – Alternate Communications Protocols

Maintain the ability to switch communication protocols while maintaining continuity of operations.

Supporting and Corporate Measures

None

1	Not used
2	• Incorporate into the contingency plans and associated training and testing the switch to alternate communications protocols (e.g. from IPv4 to IPv6). • Analyze the potential negative effects of such a switch on software applications and mitigate them.
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/CP-11

3.1.28 CP-12 – Safe Mode

"Lockdown"

Ensure that even under threat or attack the system will safeguard certain security properties.

Supporting and Corporate Measures

None

1	• Define a safe mode of operation for the system, with restrictions designed to safeguard desired properties (e.g. safety or availability) compared to the normal mode of operation. E.g. the system enters read-only mode or introduces rate-limiting for regular users. • Define the conditions for entering safe mode and for returning to normal mode.
2	Not used
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/CP-12

3.1.29 CP-13 – Alternative Security Mechanisms

"Fail-Secure"

Ensure that if the primary security mechanisms fail, the system is not left completely unprotected.

Supporting and Corporate Measures

None

1	Not used
2	• Determine the security functions that must be restored in case the primary security mechanisms fail. • Implement alternative security mechanisms for providing those security functions. They may be inferior to the primary ones (in user-friendliness, scalability, even security), but they need to be fast to deploy
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/CP-13

3.1.30 IA-2 – Identification And Authentication (Organizational Users)

Be able to assign a unique identity to each organizational user and to securely verify claims of an actor to have that identity.	
Supporting and Corporate Measures • IA-4 – Identifier Management • IA-5 – Authenticator Management • IA-6 – Authenticator Feedback • IA-7 – Cryptographic Module Authentication • IA-10 – Adaptive Identification And Authentication • IA-11 – Re-Authentication	

1	• Require users to prove their identity ("authentication") before being given access to the system or to functionalities of the system that are not designed to be publicly accessible. This is applicable to local (non-networked) access, network access (involving internal networks and VPNs) and remote access (involving external networks).
	• Consider three types of authentication factors:
	  ○ Something you know, e.g. password or PIN;
	  ○ Something you have, e.g. codes sheet, token that generates one-time-passwords;
	  ○ Something you are, e.g. biometric elements like fingerprints, face, voice.
	• For network access to privileged accounts require multifactor authentication (a combination of factors from above which do not get compromised in the same way). For other types of access use single factor authentication.

2	Same as for "1", plus: • Require multifactor authentication also for network access to non-privileged accounts and for local access to privileged accounts. • Require authentication mechanisms for network access to privileged accounts which are, besides the requirements for sophistication level "1", also replay-resistant (cannot be defeated by an attacker by recording and replaying previous authentication messages). E.g. protocols using nonces in challenges, TOTP or CRAM authenticators. • For remote access to both privileged and non-privileged accounts, require multifactor authentication with one of the factors provided by a separate device from the one gaining access. Additionally, define the strength requirements for the security mechanisms protecting the separate device.
3	Same as for "2", plus: • Require multifactor authentication also for local access to non-privileged accounts. • Require authentication mechanisms for network access to non-privileged accounts which are, besides the requirements for sophistication level "2", also replay-resistant (explanation and examples are provided in sophistication level "2").
https://nvd.nist.gov/800-53/Rev4/control/IA-2	

3.1.31 IA-3 – Device Identification And Authentication

Be able to identify devices and verify the identity of a device.

Supporting and Corporate Measures	
• IA-4 – Identifier Management • IA-5 – Authenticator Management • IA-6 – Authenticator Feedback • IA-7 – Cryptographic Module Authentication • IA-10 – Adaptive Identification And Authentication • IA-11 – Re-Authentication	
1	Not used

2	• Select the devices that truly need to support this capability, because applying this security measure to a large number of devices presents challenges.
	• A device can be authenticated using:
	  ○ Shared known information, e.g. MAC addresses of network interfaces or IP addresses of devices or cryptographic keys shared during a device registration stage.
	  ○ Organizational authentication solutions, e.g. IEEE 802.1x and EAP, Radius server with EAP-TLS, Kerberos etc.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/IA-3	

3.1.32 IA-8 – Identification And Authentication (Non-Organizational Users)

Be able to uniquely identify each non-organizational user and link actions of that user to the identity.	
Supporting and Corporate Measures	
• IA-4 – Identifier Management • IA-5 – Authenticator Management • IA-6 – Authenticator Feedback • IA-7 – Cryptographic Module Authentication • IA-10 – Adaptive Identification And Authentication • IA-11 – Re-Authentication	
1	• Require non-organizational users to prove their identity (“authentication”) when the system needs their identity (e.g. before being given access to the system or to functionalities of the system that are not designed to be publicly accessible or before accessing public functionalities for which the system needs to keep track of the users’ identities). • Consider scalability, practicality, and security in balancing the need to ensure ease of use for access to the system with the need to protect and adequately mitigate risk.
2	Same as for “1”, but with additional best practices from the Supporting Measures
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/IA-8	

3.1.33 IA-9 – Service Identification And Authentication

Be able to identify and authenticate information system services which, in a service-oriented architecture, often appear dynamically.	
Supporting and Corporate Measures	
• IA-4 – Identifier Management • IA-5 – Authenticator Management • IA-6 – Authenticator Feedback	

	• IA-7 – Cryptographic Module Authentication • IA-10 – Adaptive Identification And Authentication • IA-11 – Re-Authentication
1	• Validate the service itself or only its provider using safeguards such as: information or code signing, provenance graphs, electronic signatures attesting to the sources of the services.
2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/IA-9	

3.1.34 IR-4 – Incident Handling

Respond to incidents in a prepared, effective, constantly improved way.

Supporting and Corporate Measures

- IR-2 – Incident Response Training
- IR-3 – Incident Response Testing
- IR-5 – Incident Monitoring
- IR-6 – Incident Reporting
- IR-7 – Incident Response Assistance
- IR-8 – Incident Response Plan
- IR-9 – Information Spillage Response
- IR-10 – Integrated Information Security Analysis Team

1	• Implement an incident handling capability that covers:
	  ○ Preparation;
	  ○ Detection and analysis;
	  ○ Containment;
	  ○ Eradication;
	  ○ Recovery.
	• Coordinate incident handling activities with contingency planning activities.
	• Incorporate lessons learned from handling past incidents to improve the capability.

2	Same as for "1", plus: • Employ automated mechanisms to support incident handling.
3	Same as for "2", plus: • Correlate information from multiple incidents to observe threats whose characteristics are not distinguishable from the analysis of isolated incidents.
https://nvd.nist.gov/800-53/Rev4/control/IR-4	

3.1.35 MA-6 – Timely Maintenance

Ensure timely recovery from the malfunction or failure of components.

Supporting and Corporate Measures	
	• MA-2 – Controlled Maintenance • MA-3 – Maintenance Tools • MA-4 – Nonlocal Maintenance • MA-5 – Maintenance Personnel
1	Not used
2	• Identify the information system components whose malfunction or failure cannot be tolerated. • Put maintenance contracts in place that ensure that maintenance support and/or spare parts are obtained within a defined time from the failure.
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/MA-6	

3.1.36 MP-2 – Media Access

Ensure that certain designated types of physical storage media can only be accessed by approved persons/roles.

Supporting and Corporate Measures	
	• MP-3 – Media Marking • MP-4 – Media Storage • MP-5 – Media Transport • MP-8 – Media Downgrading
1	• Define the types of storage media (by the content they store, not by the technology) to which access must be controlled. The information may be stored digitally (e.g. optical disk, magnetic support or flash drives) or non-digitally (e.g. on paper or microfilm). • Define the persons or roles which are granted access to each type of medium defined above. • Enforce the access structure defined above through any appropriate means.
2	Same as for "1", but with additional best practices from the Supporting Measures
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/MP-2	

3.1.37 MP-6 – Media Sanitization

Ensure that no information is disclosed by remaining on information system media that is disposed, reused or released out of the control of the organization.

Supporting and Corporate Measures	
	• MP-3 – Media Marking • MP-4 – Media Storage • MP-5 – Media Transport • MP-8 – Media Downgrading

1	• Designate media which needs to be sanitized and sanitize it prior to disposal, reuse or release out of the organization's control. This includes media not readily considered "removable": media found in scanners, copiers, printers, mobile and network devices etc.
	• Choose the strength of the sanitization mechanism commensurate with the value of the confidentiality of the information potentially on the medium.
	  ○ All media can be sanitized by (partial) destruction before disposal.
	  ○ Digital media can be sanitized by e.g. clearing and cryptographic erasure.
	  ○ Non-digital media can be sanitized by e.g. redacting portions of it through obscuring them

2	Same as for "1", but with additional best practices from the Supporting Measures
3	Same as for "1", plus: • Manage the sanitization activities: review techniques, approve them, track and document actions and verify effectiveness. Tracking and documenting record personnel involved, media items sanitized and techniques used. • Periodically have a qualified and authorized external entity test the sanitization equipment and procedure. • Sanitize non-destructively storage devices between receiving them from an untrusted entity (even their manufacturer) and first connecting them to the system, thereby preventing avoidable transfers of any malicious code from those storage devices into the system.
https://nvd.nist.gov/800-53/Rev4/control/MP-6	

3.1.38 MP-7 – Media Use

"Media Use Restrictions"
Control the connection of storage media to the system to prevent unauthorized data transfer in either direction.

Supporting and Corporate Measures	
• MP-3 – Media Marking • MP-4 – Media Storage • MP-5 – Media Transport • MP-8 – Media Downgrading	

1	• Define the types of storage media whose connection to at least some components of the system must be controlled. The information may be stored on the medium digitally or non-digitally.
	  ○ Exceptions can be defined, if that does not compromise security, e.g.the medium can be connected to the sanitization equipment, approved and protected mobile devices may be connected etc.
	• Define the safeguards that will enforce the restrictions/prohibition:
	  ○ Non-technical, e.g. policies, procedures, rules of behaviour;
	  ○ Technical:
	  ▪ Physical, e.g. blocking physical access to the system or its ports, disabling or disconnecting the ports to which the storage media would be connected, etc.;
	  ▪ Logical, e.g. remove user permission to access the storage device, disable just the read or the write capability, remove the drivers needed to access the storage device etc.
	•

2	Same as for "1", plus: • Prohibit the connection of storage devices with no identifiable owner (thwarting the "flash drive found in the parking lot" attack).
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/MP-7	

3.1.39 PE-3 – Physical Access Control

Ensure that only authorized physical access is allowed to the system.

Supporting and Corporate Measures	
	• PE-2 – Physical Access Authorizations • PE-6 – Monitoring Physical Access • PE-8 – Visitor Access Records • PE-16 – Delivery And Removal

1	• Enforce authorized access at the designated entry/exit points to the facility where the (component of) the system needing protection resides:
	  ○ Verify individual access authorizations before granting access.
	  ○ Control ingress/egress to the facility.
	• Maintain audit logs for physical access.
	• Control access to areas in the facility designated as publicly accessible.
	• Have visitors escorted and their activity monitored in predetermined circumstances.
	• Handle securely any keys, access codes and other physical access devices.
	• Perform periodic inventories of physical access devices.
	• When an access device is lost, an access code is compromised or the access of individuals is curtailed, change the combinations and keys.

2	Same as for "1", but with additional best practices from the Supporting Measures
3	• In case of colocation with other information systems, enforce physical access at the level of the system, too, not only the facility in which the system resides.
https://nvd.nist.gov/800-53/Rev4/control/PE-3	

3.1.40 PE-4 – Access Control For Transmission Medium

Ensure that only authorized physical access is allowed to the transmission lines used by the system.

Supporting and Corporate Measures	
	• PE-2 – Physical Access Authorizations • PE-6 – Monitoring Physical Access • PE-8 – Visitor Access Records
1	Not used
2	• Protect the communication lines against accidental damage, disruption, tampering and eavesdropping of unencrypted communications by limiting physical access, e.g. locking wiring closets, disconnecting or locking spare network ports, conduits or cable trays for cabling. • Allow access by providing designated individuals the keys to unlock wiring cabinets, spare network ports etc.
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/PE-4	

3.1.41 PE-5 – Access Control For Output Devices

Ensure that only authorized physical access is allowed to the output devices of the system.

Supporting and Corporate Measures	
	• PE-2 – Physical Access Authorizations • PE-6 – Monitoring Physical Access • PE-8 – Visitor Access Records
1	Not used
2	• Restrict (e.g. place in a locked room) and monitor (e.g. have the access door in full view of organization personnel) physical access to the output devices. Some output devices may not be readily recognizable as such: printers/copiers, faxes, audio devices. • Allow access for designated individuals by e.g. providing them the keys to the locked room.
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/PE-5	

3.1.42 PE-9 – Power Equipment And Cabling

Secure the supply with necessary power.

Supporting and Corporate Measures	
	• PE-10 – Emergency Shutoff • PE-11 – Emergency Power • PE-12 – Emergency Lighting
1	Not used
2	• Implement the protections deemed necessary for power equipment and power cabling at internal and external locations, e.g. outside buildings: generators and power cabling; indoors: UPS and internal cabling; in self-contained entities such as vehicles: power sources.
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/PE-9	

3.1.43 PE-13 – Fire Protection

Minimize the danger posed by fires.

Supporting and Corporate Measures	
	None
1	• In facilities containing concentrations of information system resources, employ fire detection and suppression systems (e.g. handheld extinguishers, sprinklers, fixed fire hoses) with an independent energy source.
2	Same as for "1", plus: • For facilities which are not staffed continuously, employ a fire suppression system which, in addition to the requirements from sophistication level "1" is also automatic.
3	Same as for "2", plus: • Both fire detection and fire suppression systems are employed which, in addition to the requirements from lower sophistication levels, automatically notify designated personnel and emergency responders of a detection / activation.
https://nvd.nist.gov/800-53/Rev4/control/PE-13	

3.1.44 PE-14 – Temperature And Humidity Controls

Ensure that the environmental conditions are within an acceptable range.

Supporting and Corporate Measures

None

1	• Determine the acceptable temperature and humidity levels. • Employ environmental control systems that maintain the temperature and humidity in the acceptable range in the facility where the system resides. • Monitor periodically the temperature and humidity levels.
2	Not used
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/PE-14

3.1.45 PE-15 – Water Damage Protection

Prevent damage due to water leakage.

Supporting and Corporate Measures

None

1	• In facilities containing concentrations of information system resources, employ master shutoff valves or, to shut off water supplies only in the specific areas of concern, isolation valves. • Ensure that the master shutoff and/or isolation valves are accessible, working properly and known to the personnel.
2	Not used
3	Same as for "1", plus: • Employ automated mechanisms for detecting the presence of water in the vicinity of the information system and alerting the designated individuals or roles.

https://nvd.nist.gov/800-53/Rev4/control/PE-15

3.1.46 PE-17 – Alternate Work Site

Ensure appropriate safeguards in telework locations and other work locations different from the primary work location.

Supporting and Corporate Measures

None

1	Not used
2	• Define necessary, feasible and effective security controls for each alternate work site. • Ensure that personnel at the alternate work site can communicate with information security personnel in case of security incidents or problems.
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/PE-17

3.1.47 PE-18 – Location Of Information System Components

Protect the system components by choosing their position in the facility.

Supporting and Corporate Measures

None

1	Not used
2	Not used

3	• Choose the position of system components in the facility where they reside such as to minimize the potential damage from:
	  ○ Physical and environmental hazards, e.g. flooding, fire, weather phenomena, electromagnetic radiation.
	  ○ Unauthorized access caused by proximity to areas accessible to individuals not authorized physically access the components, but who might employ wireless sniffers or microphones.

https://nvd.nist.gov/800-53/Rev4/control/PE-18

3.1.48 PE-19 – Information Leakage

Prevent electromagnetic emanations through which information could be leaked.

Supporting and Corporate Measures

None

1	Not used
2	Not used
3	• Use specific techniques for avoiding or limiting electronic emanations through which information could be leaked (e.g. Faraday cages, TEMPEST proofing, zoning etc.).

https://nvd.nist.gov/800-53/Rev4/control/PE-19

3.1.49 PE-20 – Asset Monitoring And Tracking

Track the position and use of physical assets to detect their loss or inappropriate use.

Supporting and Corporate Measures

None

1	Not used
2	Not used
3	• Employ asset location technologies to track the location and movement of assets. • Ensure that the asset location technologies are employed in a way that does not breach applicable rules.

https://nvd.nist.gov/800-53/Rev4/control/PE-20

3.1.50 PL-2 – System Security Plan

Plan the use of security measures to meet the identified security requirements of the system.

Supporting and Corporate Measures	
• PL-4 – Rules Of Behavior • PL-7 – Security Concept Of Operations • PL-8 – Information Security Architecture • PL-9 – Central Management • RA-2 – Security Categorization • RA-3 – Risk Assessment	

1	• Perform a Risk Study following a methodology for risk management.
	• Additionally:
	  ○ Obtain the approval of an authorizing official prior tot he implementation of the planned measures;
	  ○ Distribute copies of the plan and of subsequent changes to defined individuals or roles;
	  ○ Periodically, or when warranted by other circumstances, review and update the security plan;
	  ○ Protect the confidentiality and integrity of the Security Plan.

2	• Coordinate the Security Plan with other organizational entities in order to reduce the impact on them of the plan's implementation.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/PL-2	

3.1.51 PS-2 – Position Risk Designation

"Organizational Role Risk Designation"	
Distinguish between the different risk levels posed by the roles existing in the organization in case of misconduct of the person occupying that role.	
Supporting and Corporate Measures	
• PS-5 – Personnel Transfer	
1	• Estimate the risk level posed by an misbehaving individual, as enabled by the organizational role of the individual. • Group the roles by similar risk levels posed and come up with a label a risk designation for each group (thereby assigning a risk designation to all organizational roles/positions), then periodically review and update those designations if necessary; • Use the risk designation of users' roles in security decisions from other Security Measures, e.g. what authorizations to grant them, how detailed the logging of their activity should be etc. • Establish screening criteria for candidates to and personnel already in those positions, e.g. training requirements, required clearances etc..
2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/PS-2 https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/position-designation-system-with-glossary-2017.pdf	

3.1.52 PS-3 – Personnel Screening

Ensure that the individuals to positions in the organisation fulfil all the mandatory requirements.	

Supporting and Corporate Measures • PS-5 – Personnel Transfer	
1	• Perform the screening of personnel prior to authorizing access to the system. • Rescreen individuals occupying a position with a certain frequency or when triggered by certain conditions established for those positions.
2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/PS-3	

3.1.53 PS-4 – Personnel Termination

Ensure that members of the organization do not continue to have unintended access rights after they cease to be members.

Supporting and Corporate Measures • PS-5 – Personnel Transfer	

1	• When individual employment is terminated, within a defined time frame:
	  ○ Revoke authorizations held by the user for the system and authenticators/credentials for accessing the system.
	  ○ Retrieve system related property from the former user.
	  ○ Conduct an exit interview in which to remind the former member of any continued security obligations extending beyond the period of employment.
	  ○ Ensure that the organization retains access to information and systems controlled by the former member.
	  ○ Notify the personnel/roles that have a need-to-know for that information.

2	Not used
3	Same as for "1", plus: • Automate the notification about the former member's departure.
https://nvd.nist.gov/800-53/Rev4/control/PS-4	

3.1.54 PS-6 – Access Agreements

Ensures user knowledge of and agreement to abide by security-related rules of behaviour.

Supporting and Corporate Measures • PS-5 – Personnel Transfer	
1	• Develop and document access agreements to protect the system, e.g. nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements • Review and update the access agreements periodically. • Make access to the system by individuals conditional on the users reading and expressing agreement to abide by the access agreements by signing them (or resigning them after they are updated or with a prescribed frequency).
2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/PS-6	

3.1.55 PS-7 – Third-Party Personnel Security

Enforce personnel security even when it comes from third-party providers.

Supporting and Corporate Measures

- PS-2 – Position Risk Designation
- PS-3 – Personnel Screening
- PS-4 – Personnel Termination
- PS-6 – Access Agreements
- PS-8 – Personnel Sanctions

1	• Establish and document personnel security requirements for personnel coming from third-party providers. • Require the third-party providers to comply with the organization's personnel security policies and procedures. • Require third-party providers to notify the organization within a given time period of any transfers or employment terminations of personnel who possesses credentials or badges or who has information system privileges. • Monitor provider compliance.
2	Not used
3	Same as for "1", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/PS-7	

3.1.56 RA-5 – Vulnerability Scanning

Verify the presence of known vulnerability types in the system.

Supporting and Corporate Measures

None

1	• Choose a scanner that uses standards to facilitate interoperation and automation.
	• Run a vulnerability scanner with a defined target scope and a defined frequency. It typically looks for:
	  ○ Whether the patch levels of the targets are up to date;
	  ○ Whether functions, ports, protocols and services are available/accessible when they should not be;
	  ○ Improper configurations;

	○ Etc. • Analyze the scan results (validate and triage findings, possibly correct the risk level of some findings). • Remediate the true positives from the scan results within the defined response time (which depends on the risk level). • Share information gleaned from the scan with other organization entities to help eliminate vulnerability types at a more systemic level.
2	Same as for "1", plus: • Use a scanning tool with the capability to update its battery of tests. • Use the update capability of the scanning tool with a certain minimum frequency or before each new scan or when new tests become available. • Give the scanning tool privileged access to scan designated targets to scan more thoroughly, e.g. exempting it from connectivity restrictions in firewalls, giving it credentials to an account, giving it credentials to a privileged account etc.
3	Same as for "2", plus: • As the scanner also reveals what information can be discovered by an adversary without mounting an attack (e.g. scanner findings with "informational" risk level, such as product names and version numbers, internal IP addresses etc.), analyse which of that information is useful only to an adversary and take steps to make it undiscoverable.
https://nvd.nist.gov/800-53/Rev4/control/RA-5	

3.1.57 RA-6 – Technical Surveillance Countermeasures Survey

"Counter-Surveillance"

Determine if the facilities where the system resides have an adequate protection against surveillance by an adversary.

Supporting and Corporate Measures

None

1	Not used
2	• Have facilities surveyed to determine: ○ Whether technical surveillance devices or hazards are present; ○ Whether the counter-surveillance measures are adequate.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/RA-6	

3.1.58 SA-3 – System Development Life Cycle

"Secure Development Lifecycle"

Build security into the information system as it is getting built.

Supporting and Corporate Measures

- SA-2 – Allocation Of Resources
- SA-5 – Information System Documentation
- SA-8 – Security Engineering Principles
- SA-10 – Developer Configuration Management
- SA-11 – Developer Security Testing And Evaluation
- SA-13 – Trustworthiness
- SA-15 – Development Process, Standards, And Tools
- SA-16 – Developer-Provided Training
- SA-17 – Developer Security Architecture And Design

	• SA-20 – Customized Development Of Critical Components • SA-21 – Developer Screening • SI-10 – Information Input Validation • SI-11 – Error Handling • SI-13 – Predictable Failure Prevention • SI-15 – Information Output Filtering • SI-16 – Memory Protection • SI-17 – Fail-Safe Procedures
1	• Use a Secure Development Lifecycle ("SDL") during development (any software development process that embeds security activities in the development activities). • Define and document the information security roles and responsibilities needed throughout the life cycle of the system. • Identify the individuals who have those roles. • Integrate a risk management process into system development life cycle activities.
2	Same as for "1", but with additional best practices from the Supporting Measures
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/SA-3	

3.1.59 SA-4 – Acquisition Process

Safeguard the system's security by imposing appropriate requirements on suppliers.

Supporting and Corporate Measures

- SA-22 – Unsupported System Components

1	• Include the following security-related requirements in the acquisition contracts for the system, components of the system or services for the system:
	  ○ Security functional requirements (capabilities, functions, mechanisms);
	  ○ Security strength requirements;
	  ○ Security assurance requirements;
	  ○ Security-related documentation requirements (on both implementation and operation);
	  ○ Requirements for protecting security-related documentation;
	  ○ Description of the development and operating environment;
	  ○ Acceptance criteria.

2	Same as for "1", plus: • Require the developer of the system/component/service to provide documentation about the functional properties (that is, properties visible at the interface) of the security controls to be employed. • Require the developer of the system/component/service to provide design/implementation information for the security controls implemented. This documentation must be of the type and the level of detail defined by the organisation based on the need to evaluate the security control. • Require the developer of the system/component/service to identify early in the development life cycle the functions, ports, protocols, and services intended to be used by the system.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SA-4	

3.1.60 SA-9 – External Information System Services

"External Service Supplier Compliance"

TBD	
Supporting and Corporate Measures None	
1	• Require providers of external information system services to comply with defined security requirements and employ defined security measures (which become "mandatory" security measures in their Risk Assessments). • Define and document oversight and responsibility roles with regards to external information system services. • Monitor the compliance of the providers on an ongoing basis.
2	Same as for "1", plus: • Require providers of external information system services to document exhaustively the list of functions/ports/protocols/services required for the provision of each of their external services.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SA-9	

3.1.61 SA-12 – Supply Chain Protection

Prevent adversaries from introducing vulnerabilities into the system at an upstream point in the supply chain.

Supporting and Corporate Measures

- SA-14 – Criticality Analysis
- SA-19 – Component Authenticity

1	Not used
2	Not used

3	• Promote threat awareness in the supply chain and in the acquisition department.
	• Use complementary, mutually reinforcing strategies to respond to risk. Aim to:
	  ○ Reduce the likelihood of unauthorized changes at every stage in the supply chain.
	  ○ Start protecting the information system (or components or services) even before the organization takes delivery. Have upstream providers do this by:
	  ▪ Protecting the development environment;
	  ▪ Vetting the personnel;
	  ▪ Using tamper-evident packaging during the shipping/warehousing of physical items.
	  ▪ Protect the documentation if required.

https://nvd.nist.gov/800-53/Rev4/control/SA-12	

3.1.62 SA-18 – Tamper Resistance And Detection

Prevent unauthorized inspection / changes to (components of) the system from being successful or from staying undetected.

Supporting and Corporate Measures	
None	
1	Not used

2	• Use technical means for tamper resistance / detection on physical artefacts related to the system to address:
	  ○ Modification or substitution by adversaries to degrade functionality or security;
	  ○ Inspection and reverse engineering by adversaries to steal know-how or to help in defeating the embedded security mechanisms.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SA-18	

3.1.63 SC-2 – Application Partitioning

Segregate the management/administrative functionality from the regular user functionality.	
Supporting and Corporate Measures	
None	
1	Not used

2	• Aim to:
	  ○ Minimise the opportunities for attackers to escalate their privileges.
	  ○ Make it possible to protect the administrative functionality more strongly.
	• Separate physically or logically the two levels of functionality by e.g. having separate URLs, separate network addresses, have them served by separate processes, run under separate system users, using virtualization techniques, running them on separate computers, etc.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-2	

3.1.64 SC-3 – Security Function Isolation

Protect security functions from interference by compromised non-security functions.	
Supporting and Corporate Measures	
None	
1	Not used
2	Not used
3	• Use an isolation boundary implemented with partitions and domains using e.g. processor rings/modes, filesystem protections, address space protections. • Restrict access to security functions from outside by using access control mechanisms and least privilege capabilities. • Try to respect as much as possible the principle that all code inside the isolation boundary is security-relevant code, although it is not always possible.
https://nvd.nist.gov/800-53/Rev4/control/SC-3	

3.1.65 SC-4 – Information In Shared Resources

"Object Reuse Prevention", "Residual Information Protection"
Prevent shared resources from becoming a pathway for smuggling information.

Supporting and Corporate Measures	
None	
1	Not used

2	• Have the system delete information (even in encrypted representation) from a shared resource between having it release by its previous user and allocating it to the next user.
	• This control does not address:
	  ○ Information remanence, where the physical medium retains traces of the information even when it has been nominally deleted.
	  ○ Covert channels, where the adversary uses operational parameters of the system as a signal carrier for information.
	  ○ Shared resources with a single user or role.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-4	

3.1.66 SC-5 – Denial Of Service Protection

Defend against attacks aiming to exhaust a limited resource needed by the system.

Supporting and Corporate Measures	
None	

1	• Define the types of denial of service attacks against which to defend the system.
	• Select and deploy the technologies that can mitigate against those types of attack. For example:
	  ○ Filtering traffic at the boundary or at the telecommunications services provider;
	  ○ Foreseeing sufficient capacity and the possibility to increase that capacity;
	  ○ Service redundancy and failover to an unaffected instance.

2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-5	

3.1.67 SC-6 – Resource Availability

"Priority Protection"

Ensure that resources are available where they are most needed.

Supporting and Corporate Measures	
None	
1	Not used
2	• Allocate resources to the most entitled consumer through a system of priorities (favouring the most entitled consumer) or quotas (preventing equally entitled consumers from consuming their fair share)
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-6	

3.1.68 SC-7 – Boundary Protection

"Perimeter Protection", "Firewall"

Define domains within which traffic is not restricted and control traffic at the boundary between domains.

Supporting and Corporate Measures	
None	
1	• Define a boundary between the system and its outside environment, as well as around internal subdomains of unrestricted communication. ○ System components which need to be both externally and internally accessible should be placed in a dedicated subnetwork separate from internal-only components. • Force communications across boundaries to pass through managed interfaces, where the communications are monitored and controlled.

2	Same as for "1", plus:
	• Limit the number of interfaces for crossing boundaries.
	• Defines an interface for each external telecommunications service and:
	  ○ Establishes a traffic flow policy through it.
	  ○ Protects the integrity and confidentiality of the traffic through it according to its security needs.
	  ○ Documents any traffic flow exceptions with a business/mission need and an expiration date.
	  ○ Periodically reviews the traffic flow exceptions list and renews or removes each exception as appropriate.
	• Use a whitelisting strategy ("deny al, permit by exception").
	• Prevent split tunnelling[8] for remote devices that have the capability to connect at the same time to internal and external resources, as such devices could be used an unauthorized interfaces for crossing boundaries.

3	Same as for "2", plus: • Route traffic from internal to external endpoints through authenticated proxy servers, which provide some insulation for the internal endpoint from the external network and where the traffic can be monitored, logged and blocked if unauthorized (by IP address, domain name, URL or analysing the content of the traffic). • Fail secure in case a boundary protection device fails. • Isolate from each other at network level system components supporting different missions and/or business functions. The isolation can be achieved through, e.g. routers, gateways, firewalls, virtualization or even through using separate encryption keys on the components supporting different missions.
https://nvd.nist.gov/800-53/Rev4/control/SC-7	

3.1.69 SC-8 – Transmission Confidentiality And Integrity

"Communication Content Protection"
Meet the confidentiality and integrity needs of information in transit.

[8] "Split tunnelling" for a remote device means the device establishing simultaneously a secured tunnel to the internal environment and a connection outside that tunnel to a non-local resource. The tunnel gives that device the same level of access as an internal device. The connection outside the tunnel turns the remote device into an interface on the boundary between the internal and external environments. However, this device is not a managed interface, therefore it undermines the boundary protection (data could be exfiltrated and malware could be infiltrated unmonitored and uncontrolled).

Supporting and Corporate Measures	
• SC-12 – Cryptographic Key Establishment And Management • SC-17 – Public Key Infrastructure Certificates • SC-20 – Secure Name / Address Resolution Service (Authoritative Source) • SC-21 – Secure Name / Address Resolution Service (Recursive Or Caching Resolver) • SC-22 – Architecture And Provisioning For Name / Address Resolution Service	
1	Not used
2	• When the transmission protections included in the telecommunications packages are insufficient, complement them with appropriate compensating controls implemented by the system itself, which can be a combination of the following: ○ Physical controls (e.g. protected distribution systems); ○ Logical controls (e.g. SC-13 – Cryptographic Protection).
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/SC-8	

3.1.70 SC-10 – Network Disconnect

Ensure that network connections do not stay open after they are not needed anymore.

Supporting and Corporate Measures	
None	
1	Not used
2	• Close connections associated with communication sessions when: ○ The session has ended, or ○ In case of connection reuse, if a new session has not started within a given time, or ○ In case of connections shared by a group of sessions, if the last remaining session of the group is in one of the first two cases.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-10	

3.1.71 SC-11 – Trusted Path

"Secure User I/O"

Ensure that sensitive user input to /output from a security function cannot be intercepted, altered or redirected by an adversary.

Supporting and Corporate Measures	
None	
1	Not used
2	Not used

3	• Provide trusted input/output paths between the user and designated security functions of the system, with the following properties:
	  ○ They protect the confidentiality and integrity of the information transmitted, even against compromised components on the same computer / network.
	  ○ They are identifiable as trusted paths (e.g. Microsoft Windows guarantees that the Ctrl+Alt+Del key combination will not be intercepted by anything else than Windows itself. Users can therefore be sure that they enter their credentials to Windows, not to a spoofed login form.) and they indicate to which security function they lead (e.g. to which security function am I authenticating now?).

https://nvd.nist.gov/800-53/Rev4/control/SC-11	

3.1.72 SC-13 – Cryptographic Protection

Provide security properties by transforming information in mathematical ways.	
Supporting and Corporate Measures	• SC-12 – Cryptographic Key Establishment And Management • SC-17 – Public Key Infrastructure Certificates

1	• Employ the appropriate standardized cryptographic technologies to obtain the desired security properties. Some examples:
	  ○ One-way transformation: e.g. hashes (for storing passwords in a way that allows using them for authentication);
	  ○ Confidentiality: e.g. encryption algorithms;
	  ○ Integrity: e.g. message authentication codes, digital signatures;
	  ○ Authenticity: e.g. authenticated encryption algorithms or modes of operation, digital signatures;
	  ○ Non-repudiation: e.g. digital signatures;
	  ○ Etc.
	• Define and document the uses of cryptography in the system and the type required for each use case.
	• Define the security parameter (e.g. key length) to be proportionate with the security needs of the information being protected (e.g. the minimum key length for information of a certain classification level).

2	Same as for "1", but with additional best practices from the Supporting Measures
3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/SC-13	

3.1.73 SC-18 – Mobile Code

Control the use of mobile code[9] in the system and the selection of mobile code technologies.

[9] Mobile code is external code which is transported onto the organization's servers and/or workstations at runtime and has therefore more potential to be malicious and attempt to cause damage than "installed" or even just "stored" code.

Supporting and Corporate Measures None	
1	Not used
2	• Define acceptable and unacceptable use cases for mobile code, e.g. document macros are an unacceptable use case, JavaScript in web pages from the same origin is an acceptable use case, Adobe Flash is an unacceptable technology because it is too hard to secure etc. • Establish usage restrictions (e.g. disable the execution of document macros on the organization's computers) and implementation guidance for acceptable mobile code (e.g. not hotlinking to the latest online version of a JavaScript library, but downloading a particular version to the organization's repository, validating that it is safe and linking to the organization's copy). • Enforce the restrictions and monitor for compliance.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-18	

3.1.74 SC-23 – Session Authenticity

Ensure that messages during a communication session come from the same party that started the session or authenticated at some point during the session.	
Supporting and Corporate Measures None	
1	Not used
2	• Ensure the authenticity of messages in a communication session (i.e. that they were created by the party that authenticated earlier, not by an attacker-in-the-middle). • Establish grounds for confidence in the ongoing identities of the other parties (i.e. that their place has not been taken over by an adversary who is replaying genuine messages captured earlier).
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-23	

3.1.75 SC-28 – Protection Of Information At Rest

Protect the confidentiality and integrity of user and system information while it is stored.	
Supporting and Corporate Measures • SC-12 – Cryptographic Key Establishment And Management • SC-17 – Public Key Infrastructure Certificates	
1	Not used

2	• Select and use the most appropriate available technique. Among the possibilities are:
	  ○ SC-13 – Cryptographic Protection (confidentiality and integrity);
	  ○ Scanning for file integrity (integrity);
	  ○ Recording information on WORM media (integrity);
	  ○ Storing information in secure offline storage (confidentiality and integrity).

3	Same as for "2", but with additional best practices from the Supporting Measures
https://nvd.nist.gov/800-53/Rev4/control/SC-28	

3.1.76 SC-31 – Covert Channel Analysis

Identify and characterize potential areas of the system that are not meant to carry information, but might nevertheless be used as a signal carrier.

Supporting and Corporate Measures

None

1	Not used
2	Not used

3	• Involve developers in identifying the potential for problematic covert channels:
	  ○ Covert channels can be of two types: timing (e.g. the adversary sender can influence the system's response time to a request and the recipient adversary derives the intended information from the measurements of the response time) or storage (e.g. the adversary sender can control the size of a file and the recipient adversary can monitor that size even though the recipient cannot read the content of the file).
	  ○ Problematic channels are those that are capable of signalling across security domains (in networks or across security levels on one computer).
	• Estimate the maximum bandwidth of the identified types of covert channels.

https://nvd.nist.gov/800-53/Rev4/control/SC-31

3.1.77 SC-34 – Non-Modifiable Executable Programs

Prevent the modification of the software loaded for execution.

Supporting and Corporate Measures

None

1	• Launch the operating environment and designated applications from hardware-enforced read-only media, such as non-rewritable optical media or one-time programmable read-only memory.(Reprogrammable read-only memory is also accepted if it can be ensured that it cannot be reprogrammed by an adversary between the correct writing and the insertion into the system, nor while it is in the system).
2	Not used
3	Not used

https://nvd.nist.gov/800-53/Rev4/control/SC-34

3.1.78 SC-39 – Process Isolation

Prevent processes from interfering with or tampering with other processes.

Supporting and Corporate Measures	
None	
1	• Use operating system or virtualization capabilities to ensure that processes communicate with each other only in a manner controlled by the security functions (which enforces documented abstractions like isolation and access permissions). • Develop the capabilities mentioned in the previous point if this system itself implements the concept of process.
2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-39	

3.1.79 SC-40 – Wireless Link Protection

Prevent a multitude of attacks against the wireless link.

Supporting and Corporate Measures	
• SC-12 – Cryptographic Key Establishment And Management • SC-17 – Public Key Infrastructure Certificates	
1	Not used
2	• Analyze the attacks that could be mounted by adversaries against the internal or external wireless links of this system with all its particularities (e.g. gain intelligence, perform jamming, spoof legitimate users). Note that if the wireless links are commodity transmission services of commercial service providers it might not be possible to implement this measure.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SC-40	

3.1.80 SI-2 – Flaw Remediation

"Security Patching"

Manage the vulnerabilities linked to announced flaws in supplier-provided system components and the remediation through supplier provided security updates.

Supporting and Corporate Measures	
None	

1	• Identify the extent to which the system is impacted by announced flaws (e.g. from security advisories).
	• Correct the flaws when a remediation is made available:
	  ○ React in a timely manner to the publication of a remediation.
	  ○ Test the remediation, if warranted, before deploying it widely to ensure that it is effective and does not have unwanted side effects (e.g. roll it out progressively through the development, testing, acceptance and then production environments).
	• Integrate flaw remediation with measure CM-9 – Configuration Management Plan.

2	Same as for "1", plus: • Automate the reporting of the flaw remediation status.
3	Same as for "2", plus: • Manage flaw remediation centrally (planning, implementing, assessing, authorizing and monitoring the flaw remediation controls).
https://nvd.nist.gov/800-53/Rev4/control/SI-2	

3.1.81 SI-3 – Malicious Code Protection

"Antivirus", "Anti-malware"
Neutralize malware that managed to arrive on the system's computers.

Supporting and Corporate Measures	
None	

1	• Employ malware detection and eradication mechanisms at the system's entry and exit points to prevent "contagion" (e.g. on the network boundary, at connection points for mobile devices etc.)
	• Employ malware detection and eradication mechanisms on the information system itself:
	  ○ At the moment when malware would transition to and from memory or storage (e.g. when downloading information, when reading a file for visualization or execution etc.)
	  ○ Scan the system (memory and storage), e.g. looking for malware that was not yet known when the malware crossed any of the checkpoints listed above.
	• Ensure that the protection mechanisms get updated to the newest available releases in a timely fashion.
	• React to the detection of malware with the response decided by the organization. Several possibilities are:
	  ○ Alert the administrators;
	  ○ Quarantine the malware (prevent it from being inadvertently executed or copied);
	  ○ Delete it.
	• Prepare for the eventuality of a false positive detection which may impact the availability of files necessary for the system's operation e.g. detecting an essential system file as malware and deleting it, crippling the system.

2	Same as for "1", plus: • Manage malicious code protection centrally (planning, implementing, assessing, authorizing and monitoring the flaw remediation controls). • Enable automatic updates of the protection mechanisms (e.g. auto-update virus signatures database or detection rules).
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SI-3	

3.1.82 SI-4 – Information System Monitoring

"Intrusion Detection", "Security Information and Event Management", "Security Monitoring"

Make the defenders of the system aware of adversary activity against the system.

Supporting and Corporate Measures	
None	
1	• Build monitoring and analysis functions into the system to help detect attacks, attack attempts, unauthorized connections to the system (local, network or remote) and unauthorized use of the system. • Deploy stand-alone monitoring devices at strategic points to collect essential information or at ad-hoc locations to track specific types of transactions. • Protect the monitoring information's confidentiality, integrity and availability. • Adjust the thoroughness of the monitoring in accordance with the organization's threat level. • Only carry out monitoring activities deemed lawful after obtaining a legal opinion. • Inform stakeholders of the monitoring results on a need-to-know basis and with a predetermined frequency.
2	Same as for "1", plus: • Use automated tools for real-time analysis of the events detected by monitoring. • Monitor inbound and outbound traffic for indicators of malicious activity. • Generate alerts when predetermined conditions occur.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SI-4	

3.1.83 SI-5 – Security Alerts, Advisories, And Directives

Handle the flow of security alerts, advisories and directives[10] in a systematic way.	
Supporting and Corporate Measures	
None	
1	• Receive security alerts, advisories and directives from predetermined sources on an ongoing basis. • Generate internal security alerts, advisories and directives as needed. • Disseminate security alerts, advisories and directives internally and externally on a need-to-know basis. • Implement security directives in a timely fashion or notify the issuing organization about the noncompliance.
2	Not used
3	Same as for "1", plus: • Disseminate security alert and advisory information throughout the organization using automated mechanisms.
https://nvd.nist.gov/800-53/Rev4/control/SI-5	

3.1.84 SI-7 – Software, Firmware, And Information Integrity

"Integrity Checking"
Prevent modifications to essential system information from staying undetected.
Supporting and Corporate Measures
None

[10] Security alerts, advisories and directives are notifications about current attack campaigns, technological change (e.g. removal of support for deprecated security technology) and other non-vulnerability information (which are dealt with by measure SI-2 – Flaw Remediation)

1	Not used

2	• Designate the pieces of system information which need integrity, e.g.:
	  ○ Operating system components, middleware, applications (software);
	  ○ A PC's BIOS, software embedded in a special purpose device (firmware);
	  ○ A file's owner, permissions, creation/access/modification times (information).
	• Provide the capability to check the integrity of the chosen information, e.g. through parity checks, cyclic redundancy checks, cryptographic hashes.
	• Perform the integrity checks in predetermined circumstances, e.g. at startup, with a given frequency, when certain events occur (installation, update etc.).
	• Integrate the integrity check into the organization's incident response capability.

3	Same as for "2", plus: • Generate automatic notifications of integrity violations. • Automate predetermined responses to given integrity violations, e.g. system shutdown, destruction and replacement of a container with a clean copy. • Prohibit (with exceptions only for compelling reasons) the use of binaries from sources that provide no or only limited warranty and do not provide the source code.
https://nvd.nist.gov/800-53/Rev4/control/SI-7	

3.1.85 SI-14 – Non-Persistence

"Ephemeral Components"

Reduce the duration of persistence of adversaries in the system by designing the components to have limited lifetime, after which they get replaced with clean instances.

Supporting and Corporate Measures

None

1	Not used
2	• Design the system to work even when components are frequently restarted to a known good state • Restart the components frequently to the known good state, as this will withdraw adversary control over those components and force the attacker to spend more effort on simply trying to achieve persistence in the system.
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/SI-14	

3.2 Supporting Measures

The measures in this section are applied at the level of the Communication and Information System. They do not achieve a reduction in the likelihood or impact of a risk scenario, but contribute to the success of Mitigating Measures from the previous section.

3.2.1 AC-2 – Account Management

Manage the life cycle of the in-system identity of its users and groups of users.

1	• Design the account and roles structure for the system (e.g. administrators, editors and readers). • Carry out account creation, modification, enabling/disabling and removal under the conditions and following the procedures defined for that.

	• Monitor and audit the use of the accounts. • Review the accounts with a predefined frequency. • If the system uses group accounts, ensure a procedure for reissuing group account credentials when a member of the group leaves the group.
2	Same as for "1", plus: • Support the management of accounts with an automated system. • Automate the removal of temporary accounts after a predetermined time. • Automate the disabling of accounts after a predefined period of inactivity. • Automate the auditing of account creation, modification, enabling/disabling and removal and automate the notification of the appropriate roles when problems are found.
3	Same as for "2", plus: • Require users to log out of their account after a period of inactivity or when other circumstances are met that would put the authenticity of their login sessions at risk. • Have the system enforce the usage conditions of the accounts (e.g. usable only during working hours). • Have the system monitor accounts for atypical usage (defined however it is meaningful for the system) and report atypical usage to predefined individuals or roles.
https://nvd.nist.gov/800-53/Rev4/control/AC-2	

3.2.2 AC-5 – Separation Of Duties

Reduce the risk of solitary abuse of authorized privileges by making sensitive workflows require the involvement of multiple people and mutual checks.

1	Not required
2	Same as for "3"
3	• Design and document the workflows that require separation of duties to include distinct roles and responsibilities. • Define authorizations in the system to support the separation of duties in the workflows above.
https://nvd.nist.gov/800-53/Rev4/control/AC-5	

3.2.3 AC-6 – Least Privilege

Reduce the risk of abuse of authorized privileges by granting users only the privileges needed to accomplish their assigned tasks.

1	Not required
2	• Grant privileges to users and information system processes only to the extent that they need them to accomplish their assigned tasks / required functions. • Require explicit authorization for access to security-relevant information or security functions of the system. • Create privileged accounts (e.g. super user, system administrator, root) only for a limited subset of the users. • Prohibit non-privileged accounts from accessing security-relevant information or security functions of the system. • Require users to only use their privileged accounts or roles when accessing security-relevant information or security functions of the system, but not when accessing non-security functions.

	• Audit the use of privileged functions and report misuse to predefined individuals or roles.
3	Same as for "2", plus: • Only allow network access to security functions of the system for compelling operational needs. Document that rationale in the security plan for the system.
https://nvd.nist.gov/800-53/Rev4/control/	

3.2.4 AC-7 – Unsuccessful Logon Attempts

"Defence Against Password Brute Force Attacks"	
Reduce the risk due to adversaries repeatedly attempting to log in as other legitimate users.	
1	Same as for "2"
2	Same as for "3"

3	• Define a limit on the number of successive failed login attempts during a given period of time which can be considered "honest mistakes".
	• Slow down any further login attempts by one of the following measures by the system when the limit is exceeded:
	  ○ Delay the response to further login attempts according to a predefined algorithm that has the effect of drastically reducing the login attempt rate for the adversary.
	  ○ Block the account (deny access even if the correct credentials are presented), for a predefined amount of time or until an administrator unblocks it.
	When defining the parameters above, take into account the potential for denial of service by preventing/delaying legitimate user login.

https://nvd.nist.gov/800-53/Rev4/control/AC-7	

3.2.5 AC-8 – System Use Notification

Display for the users a privacy and security notice when they log in to the system.	
1	Same as for "2"
2	Same as for "3"
3	• Display the notice before granting access to the system. • Require users to acknowledge the notice and take explicit action to continue.
https://nvd.nist.gov/800-53/Rev4/control/AC-8	

3.2.6 AC-9 – Previous Logon (Access) Notification

Facilitate detection by the user of previous fraudulent logins to their account.	
1	Same as for "2"
2	Same as for "3"
3	• Upon successful login to the system, display to the user the date and time of the last successful login to their account.
https://nvd.nist.gov/800-53/Rev4/control/AC-9	

3.2.7 AC-10 – Concurrent Session Control

Limit the number of concurrent sessions allowed.	
1	Not required
2	Same as for "3"
3	For certain predefined accounts or account types (e.g. administrators, users working in sensitive domains, managers or everybody) if the number of concurrent sessions for an account has reached the predefined limit, terminate the oldest session before allowing the login.
https://nvd.nist.gov/800-53/Rev4/control/AC-10	

3.2.8 AC-11 – Session Lock

Suspend access to the system while keeping the session intact.	
1	Not required
2	Same as for "3"

3	• Prevent access to the system as part of an established session until the user authenticates again, if one of the following conditions occurs:
	  ○ A predetermined duration of inactivity has occurred;
	  ○ The user requests that the system locks the session.
	• If the session is associated with output on a display, obscure for the duration of the lock the information that was previously visible.

https://nvd.nist.gov/800-53/Rev4/control/AC-11	

3.2.9 AC-12 – Session Termination

Forcibly terminate a logical session under predefined conditions.	
1	Not required
2	Same as for "3"

2	• Have the ability for the system to trigger the end a user's logical session (e.g. terminate all running system processes the user initiated during the session, except those specifically created to outlast the logical session).
	• Trigger the session termination at the initiative of the system when predefined conditions are met, for example:
	  ○ A period of user inactivity has reached a predefined threshold;
	  ○ Malicious activity has been detected in the session;
	• Time-based conditions are met (e.g. office hours ended, a public holiday started etc.).

https://nvd.nist.gov/800-53/Rev4/control/AC-12	

3.2.10 AC-14 – Permitted Actions Without Identification Or Authentication

"Anonymous Actions"	
Foresee anonymous actions that are consistent with the system's mission/business functions.	
1	Same as for "2"
2	Same as for "3"

3	• Define and document the actions a user can take on the system without being required to authenticate, which will be allowed because, e.g. they increase engagement without lowering security.
https://nvd.nist.gov/800-53/Rev4/control/AC-14	

3.2.11 AC-16 – Security Attributes

"Security Metadata"	
Accompany business data with security-relevant details.	
1	Same as for "2"
2	Same as for "3"
3	• Define a set of security-relevant data that can be associated with business data items, e.g. confidentiality classification for a file, clearance level for a user, document creator, owning project etc. • Ensure that predefined security attributes accompany predefined business data items as these are stored, transmitted and processed. • Make the security attributes available to the system's security functions, e.g. to access control, to system monitoring etc.
https://nvd.nist.gov/800-53/Rev4/control/AC-16	

3.2.12 AC-22 – Publicly Accessible Content

Control publicly accessible content to prevent the disclosure of non-public information.	
1	Same as for "2"
2	Same as for "3"
3	• Designate and train the individuals allowed to publish public information. • Review content about to be posted publicly to ensure it does not contain non-public information. • Review content already publicly accessible to detect and remove non-public information.
https://nvd.nist.gov/800-53/Rev4/control/AC-22	

3.2.13 AC-24 – Access Control Decisions

Take correct decisions whether to allow an access attempt or not.	
1	Same as for "2"
2	Same as for "3"

3	• Have the ability to decide whether to allow an access attempt or not, based on:
	  ○ The parameters of the access (including the security attributes involved);
	  ○ An access policy (the rules on what to allow and what not)
	• Embed the ability to take access control decisions in the same entity that enforces the access decision or in a separate one, depending on what is optimal for the system.

https://nvd.nist.gov/800-53/Rev4/control/AC-24	

3.2.14 AC-25 – Reference Monitor

Access functions or resources not directly, but through a mediator component (the "reference monitor") that enforces access rules.	
1	Same as for "2"
2	Same as for "3"

3	• Mediate access to resources through a component that enforces access rules with the following additional properties:
	  ○ It is tamperproof, to prevent it from being corrupted;
	  ○ It is always invoked, to prevent access enforcement from being bypassed.
	• It is small enough that assurance of correctness can be obtained through complete analysis and testing.

https://nvd.nist.gov/800-53/Rev4/control/AC-25	

3.2.15 AT-4 – Security Training Records

At organization level, keep track of who received what security training.	
1	Same as for "2"
2	Same as for "3"
3	• Create and retain for a predefined period individual training records, including security awareness training and specific security training.
https://nvd.nist.gov/800-53/Rev4/control/AT-4	

3.2.16 AU-3 – Content Of Audit Records

Specify the content of the audit records the System creates.	
1	• Record the necessary information to allow for the reconstruction of events, e.g. time stamps, source and destination network addresses, user, process IDs, resources, access control rules involved in access decisions, the outcome of access control decisions etc.
2	Same as for "1", plus: • Record additional information, complementary to the minimally necessary information, e.g. if needed for specific audit requirements. E.g. recording of the I/O of privileged commands, individual identity of member using a group account.
3	Same as for "2", plus: • Manage centrally and dynamically the content of audit records generated by predefined components of the System, e.g. through automation or configuration management.
https://nvd.nist.gov/800-53/Rev4/control/AU-3	

3.2.17 AU-4 – Audit Storage Capacity

Avoid reduction of auditing capability caused by running out of storage capacity for the audit records.	
1	Same as for "2"
2	Same as for "3"

3	• Estimate the storage capacity needs for audit records taking into account the foreseen activity, intended content of audit records, and audit processing requirements. • Allocate sufficient storage capacity to satisfy at least the foreseen storage needs estimated above.
https://nvd.nist.gov/800-53/Rev4/control/AU-4	

3.2.18 AU-5 – Response To Audit Processing Failures

Define in advance the appropriate response to failures in audit processing.	
1	Same as for "2"

2	• Detect audit processing failures and alert predefined individuals and roles.
	• Take a predefined response to audit processing failures, such as:
	  ○ Shut down System;
	  ○ Overwrite oldest audit records;
	  ○ Stop generating new audit records;
	  ○ Etc.

3	Same as for "2", plus: • Alert predefined individuals and roles when a predefined threshold of the audit record storage capacity has been reached (expressed as a fixed amount below maximum capacity or as a fraction of the maximum capacity). • Perform the aforementioned alerting in real-time for predefined types of alerts.
https://nvd.nist.gov/800-53/Rev4/control/AU-5	

3.2.19 AU-6 – Audit Review, Analysis, And Reporting

Use the audit trail in the detection of inappropriate or unusual activity.	
1	• Have an organization entity with the appropriate authority review and analyse the audit trail to detect inappropriate or unusual activity. • Report the detected instances of such activity to predefined individuals and roles.
2	Same as for "1", plus: • Use automated mechanisms to integrate audit review and analysis with the organization's other investigative processes. • Correlate this measure across different audit record repositories to get the bigger picture.

3	Same as for "2", plus:
	• Integrate this measure with the review, analysis and reporting of information produced by other processes, such as:
	  ○ Vulnerability scanning;
	  ○ Performance measurement;
	  ○ Information system monitoring;
	  ○ Etc.
	• Integrate this measure with physical monitoring (e.g. does the surveillance camera footage confirm that the individual using a badge was indeed the legitimate user?).

https://nvd.nist.gov/800-53/Rev4/control/AU-6	

3.2.20 AU-7 – Audit Reduction And Report Generation

Possess the capability to analyze the audit trail in an automatable and safe way.	
1	Not required
2	Same as for "3"
3	• Support on-demand audit trail processing for analysis and reporting purposes, e.g. data mining, filtering. • Ensure that the original audit trail is not altered (neither in content, nor in the order of records). • Automate the capability to process a subset of the audit trail based on predefined fields of the audit records.
https://nvd.nist.gov/800-53/Rev4/control/AU-7	

3.2.21 AU-8 – Time Stamps

Use a reliable way to map audit events to time moments.	
1	• Use an internal clock to generate time stamps (date and time) with a predefined minimum granularity (precision) and accuracy (degree of closeness between the system clock and reference clocks). • Save as part of the audit record a time stamp that can be mapped to UTC, so the time stamps from different internal clocks can be compared.
2	Same as for "3"
3	Same as for "1", plus: • Synchronize the system's clock with a predefined authoritative time source, e.g. manually, in a custom automated way, using NTP etc. This usually involves: 1. Comparing the system's clock with the time source with a predefined frequency (this limits the amount of clock drift). 2. Correcting the system's clock when the drift exceeds a predefined threshold (this limits the number of time "jumps").
https://nvd.nist.gov/800-53/Rev4/control/AU-8	

3.2.22 AU-9 – Protection Of Audit Information

Maintain the confidentiality, integrity and availability of the audit capability.	
1	• Protect the audit information and the audit tools with technical measures against unauthorized access, modification and deletion.
2	Same as for "1", plus: • Limit the authorized access to audit information and tools to a subset of privileged users.
3	Same as for "2", plus: • Keep backups of the audit information on a separate physical system or component than the system or component being audited. • Use cryptographic mechanisms to protect the audit information and tools against undetected unauthorized modification.
https://nvd.nist.gov/800-53/Rev4/control/AU-9	

3.2.23 AU-11 – Audit Record Retention

Keep audit records as long as needed and required.	
1	Same as for "2"
2	Same as for "3"
3	• Retain the audit records until they are not needed for any administrative, legal, audit or operational purpose. • Predefine standard categories of audit records for the different retention duration needs (e.g. user activity records, connectivity records etc.)
https://nvd.nist.gov/800-53/Rev4/control/AU-11	

3.2.24 AU-12 – Audit Generation

Have events of interest leave an audit trail.	
1	Same as for "2"
2	• Provide the capability to selectively enable audit record generation for the desired types of audit events among those that the system or component is capable of recording. • Generate audit records during operation for the selected event types.
3	Same as for "2", plus: • Aggregate audit records from multiple logs into a time-correlated audit trail (one in which a time ordering of the records from different logs can be achieved within allowable tolerances). • Allow authorized individuals to adjust (extend or limit) the level of logging based on predefined criteria.
https://nvd.nist.gov/800-53/Rev4/control/AU-12	

3.2.25 AU-14 – Session Audit

Have the capability to follow in real time or record the activity in a user session.	
1	Same as for "2"
2	Same as for "3"
3	• Prepare and carry out session audits in consultation with legal counsel to ensure lawfulness. • Provide the capability to follow and record user activity, e.g. keystrokes, commands executed, web sites visited, information/files transferred etc.
https://nvd.nist.gov/800-53/Rev4/control/AU-14	

3.2.26 AU-15 – Alternate Audit Capability

Have a backup auditing capability.	
1	Not required
2	Same as for "3"

3	• Foresee a fall-back audit capability:
	  ○ To use in case the primary auditing capability fails;
	  ○ To use until the primary capability is restored;
	• Possibly providing only a predefined subset of the functionality of the primary audit capability.

https://nvd.nist.gov/800-53/Rev4/control/AU-15	

3.2.27 AU-16 – Cross-Organizational Auditing

Coordinate the approach to auditing when it must be performed across organizational boundaries.	
1	Same as for "2"
2	Same as for "3"
3	• Foresee and apply methods to ensure that audit information from other organizations (e.g. SaaS) can be consumed and audit information provided to other organizations can be consumed by them. An example of audit information in need of coordination is user identity.
https://nvd.nist.gov/800-53/Rev4/control/AU-16	

3.2.28 CA-5 – Plan Of Action And Milestones

Remedy vulnerabilities and weaknesses in a planned way.	
1	Same as for "2"
2	Same as for "3"

3	• Plan (with milestones) the remediation actions resulting from activities such as the ones below, that can reveal vulnerabilities, weaknesses and security deficiencies:
	  ○ CA-2 – Security Assessments;
	  ○ CA-8 – Penetration Testing;
	  ○ RA-5 – Vulnerability Scanning;
	  ○ CA-7 – Continuous Monitoring;
	  ○ Etc.
	• Update the plan to keep up with the information provided by the activities above.

https://nvd.nist.gov/800-53/Rev4/control/CA-5	

3.2.29 CA-6 – Security Authorization

Ensure that the system enters operation only with proper management approval.	
1	Same as for "2"
2	Same as for "3"
3	• Assign a senior-level executive as authorizing official. • Require the authorizing official's authorization before commencing operations. Risk information needs to be provided for decisional support. • Require re-authorization with a predefined frequency to continue operations. Risk information needs to be provided for decisional support.
https://nvd.nist.gov/800-53/Rev4/control/CA-6	

3.2.30 CA-7 – Continuous Monitoring

Make the defenders of the system aware of the system's current state and behaviour.

1	• Develop a monitoring strategy and implement a continuous monitoring program consisting of:
	  ○ Specifications of what metrics to measure, where and how often;
	  ○ Control assessments to ensure that the needed metrics are collected;
	  ○ Procedures to correlate and analyze the measured metrics;
	  ○ Response actions to be taken under predefined outcomes of the analysis;
	  ○ Reporting to the predefined individuals or roles of predefined information obtained from monitoring and from analysis.

2	Same as for "3"
3	Same as for "1", plus: • Employ independent assessors to monitor the system's security controls.

https://nvd.nist.gov/800-53/Rev4/control/

3.2.31 CM-3 – Configuration Change Control

Ensure that configuration changes are managed.

1	Not required

2	• For predefined types of changes, put in place a process which ensures that:
	  ○ Configuration changes are implemented only after approval.
	  ○ Approval for a change is provided only after it is reviewed by an appointed body (e.g. "Change Management Board"), which is convened with predefined frequency and which also provides oversight and coordination of the process.
	  ○ The review takes into account security impact and is performed on a standardised documentation of every change.
	  ○ Every change is tested and validated before being implemented on the operational system.
	  ○ Retain for a predefined period records of the configuration changes.
	  ○ Audit and review configuration change control activities.

3	Same as for "2", plus:
	• Use automated mechanisms for:
	  ○ Change documentation (proposed and implemented);
	  ○ Approval request;
	  ○ Prohibition of the implementation of not (yet) approved changes;
	  ○ Notification of completion.

https://nvd.nist.gov/800-53/Rev4/control/CM-3

3.2.32 CM-4 – Security Impact Analysis

Anticipate the security impact of proposed changes to the system.

1	Same as for "2"
2	• Designated individuals / roles with the required skills and expertise (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) analyse the security ramifications of the proposed changes, including the impact on existing security measures and whether the parameters of the tracked risk scenarios change or new risk scenarios are introduced.

3	Same as for "2", plus: • Changes are tested in a separate, dedicated environment prior to being implemented in an operational environment.
https://nvd.nist.gov/800-53/Rev4/control/CM-4	

3.2.33 CM-5 – Access Restrictions For Change

Treat changes to the system as security-sensitive actions.	
1	Not required

2	• Restrict the set of individuals / roles authorized to implement changes to the system and ensure that only qualified individuals are authorized.
	• Enforce access restrictions on the change actions, e.g.:
	  ○ Physical and logical access control;
	  ○ Workflow automation;
	  ○ Media libraries;
	  ○ Abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems);
	  ○ Change windows (e.g., changes are scheduled only during specified times, when the activity can be better monitored and any change outside of the window is automatically suspicious).
	• Keep an audit trail of the change-related actions to be prepared for an after-the-fact investigation in case unauthorized changes are discovered.

3	Same as for "2", plus: • Automate the access enforcement and the audit trail. • Review with a predefined frequency the history of system changes to determine whether unauthorized changes have occurred. • For a predefined subset of software components to be installed, only accept digitally signed code with a signature from the component's pre-approved trusted source.
https://nvd.nist.gov/800-53/Rev4/control/CM-5	

3.2.34 CM-6 – Configuration Settings

Manage the set of configurable parameters of the system.	
1	Same as for "2"
2	• Establish, document and implement the "lowest privilege" values for the settings of the system, that are consistent with operational requirements. • Manage deviations from these values: identify, document and approve the deviations. • Monitor and control the changes to the previous two categories of information.
3	Same as for "2", plus: • Use automation to manage/apply and verify configuration settings. • Establish safeguards to respond to unauthorized changes to the configuration settings.
https://nvd.nist.gov/800-53/Rev4/control/CM-6	

3.2.35 CM-7 – Least Functionality

"Hardening", "Lock-down"

Reduce the attack surface through eliminating unneeded capabilities.	
1	• Configure the system to only provide the capabilities needed for carrying out its business/mission function, preferably a single function per device. • Maintain a list of out-of-the-box capabilities of the components, which are prohibited and need to be deactivated or restricted, e.g. functions, ports, protocols, services etc.
2	Same as for "1", plus: • Review with a predefined frequency the system to identify and disable unnecessary or insecure capabilities. • Prevent arbitrary program execution in accordance to a predefined policy and restrictions (e.g. launched by authorized users, running during authorized time windows etc.). • Blacklist unauthorized software (allow by default, deny if listed).
3	Same as for "2", with the following changes: • Instead of blacklisting unauthorized software, whitelist authorized software (deny by default, allow if listed).
https://nvd.nist.gov/800-53/Rev4/control/CM-7	

3.2.36 CP-3 – Contingency Training

Train users for contingencies.	
1	Same as for "2"

2	• Provide users contingency training and require them to follow it:
	  ○ Consistent with assigned roles and responsibilities;
	  ○ Within a predefined time after assuming their role;
	  ○ Afterwards, when the system changes warrant it or with a predefined frequency, whichever occurs first.

3	Same as for "2", plus: • Use simulated events in the training.
https://nvd.nist.gov/800-53/Rev4/control/CP-3	

3.2.37 CP-4 – Contingency Plan Testing

Ensure that contingency planning is effective by testing it.	
1	• Define and carry out tests for validating the effectiveness of the contingency plans. • Review the test results and initiate any needed actions to improve the effectiveness of the contingency plans.
2	Same as for "1", plus: • Coordinate the testing of the contingency plans with related plans, e.g. Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans.
3	Same as for "2", plus: • Test contingency plans at the alternate site, too (also see 'CP-6 – Alternate Storage Site' and 'CP-7 – Alternate Processing Site').
https://nvd.nist.gov/800-53/Rev4/control/CP-4	

3.2.38 CP-10 – Information System Recovery And Reconstitution

Include in the contingency plans the return to a known good state through recovery and reconstruction of the system.

1	• Plan to follow up recovery (restoration of the system's function) with reconstruction (return to fully operational):
	  ○ Prepare the system against future disruptions, compromises or failures.
	  ○ Resume not only the business functions, but also the security functions, e.g. perform the necessary reauthorizations, continuous monitoring etc.
	  ○ Deactivate the interim system capabilities as the permanent capabilities take over.

2	Same as for "1", plus: • Perform transaction recovery for transaction-based systems, e.g. perform transaction rollback, replay of transaction journals etc.
3	Same as for "2", plus: • Have an upper time limit for the restoration.

https://nvd.nist.gov/800-53/Rev4/control/CP-10

3.2.39 IA-4 – Identifier Management

Ensure that identifiers used by the system have the needed properties.

1	Same as for "2"
2	Same as for "3"

3	• Have a system for selecting identifiers (e.g. user names, MAC addresses, IP addresses etc.) which governs:
	  ○ The selection of identifiers (e.g. rules such as "for user names, the first 5 letters of the family name, followed by the first 2 letters of the first name");
	  ○ The assignment of identifiers, with any corresponding approval process;
	  ○ The prevention of identifier reuse during a predefined cooldown period;
	  ○ The disabling of the identifier.

https://nvd.nist.gov/800-53/Rev4/control/IA-4

3.2.40 IA-5 – Authenticator Management

"Credentials Management"

Manage the lifecycle of the elements used to authenticate entities in the system.

1	• Before associating an authenticator to an entity (by distributing it, by having a user choose their password etc,), verify the identity of that entity in some other way.
	• Ensure a strength of the authenticator commensurate with their intended use, e.g. password length, maximum lifetime.
	• Have administrative procedures for the initial authenticator distribution, for replacement of lost/compromised/damaged authenticators, as well as for revocation. For example:
	  ○ Do not use well-known default passwords.
	  ○ Require the initial password to be changed.
	  ○ Never transmit the password unprotected over the network.
	  ○ Inform the recipient of their duty to protect the authenticator (even giving specific ways).
	  ○ Change group authenticators when an individual leaves the group.
	  ○ Etc.

	• Define a policy for passwords, if they are used. • Define a policy for hardware tokens, if they are used.
2	Same as for "3"
3	Same as for "1", plus: • Define a policy for PKI-based authentication (also for other PKI authenticators than hardware tokens). • Require the recipient to be present in person when receiving an authenticator or to delegate a trusted third-party.
https://nvd.nist.gov/800-53/Rev4/control/IA-5	

3.2.41 IA-6 – Authenticator Feedback

"Shoulder Surfing Protection"	
Ensure that system feedback during authentication does not compromise the authenticator.	
1	Same as for "2"
2	Same as for "3"
3	• When the system provides feedback of the use of an authenticator, ensure a good balance between user-friendliness (e.g. show asterisks instead of the password symbols entered to confirm that the symbol was received) and security (e.g. do not show the password in full, especially on a big desktop screen). • Adapt the balance to the specific scenario of using the authenticator, e.g. on the small screen of a mobile device which can be shielded from prying eyes, show the last entered password symbol for a few seconds to allow for the correction of typos caused by the less precise on-screen keyboard.
https://nvd.nist.gov/800-53/Rev4/control/IA-6	

3.2.42 IA-7 – Cryptographic Module Authentication

"Cryptographic Module Access Control"	
Allow a cryptographic module to be used only in authorized ways.	
1	Same as for "2"
2	Same as for "3"
3	• Require the user of a cryptographic module to authenticate to the module to prevent cryptographic operations (e.g. decryption, creation of a digital signature) from being misused. • Allow even authenticated users of the cryptographic module to perform only the functions they are authorized to perform.
https://nvd.nist.gov/800-53/Rev4/control/IA-7	

3.2.43 IA-10 – Adaptive Identification And Authentication

Adapt the strength of authentication mechanism to the circumstances of each authentication act.	
1	Same as for "2"
2	Same as for "3"

3	• Foresee different strengths of mechanism for the authentication required in different conditions, such as:
	  ○ Stronger authentication when there is suspicion that the regular credentials may have been compromised, e.g. when the access is from a potentially hostile location or at an atypical time of day;
	  ○ Stronger authentication when higher sensitivity (or quantity) access is attempted, e.g. to security functionality or to a large number of records;
	• Weaker, but more user-friendly, authentication when low-sensitivity access is attempted, e.g. read-only access.

https://nvd.nist.gov/800-53/Rev4/control/IA-10	

3.2.44 IA-11 – Re-Authentication

Require the users to re-authenticate in circumstances where security requires it (besides unlocking a locked session).

1	Same as for "2"
2	Same as for "3"

3	• Require the user to (re-)enter the current credentials in predefined situations, e.g.:
	  ○ When authenticators were changed;
	  ○ When roles were changed;
	  ○ When the security categories of the accessed information or functions changed;
	  ○ When a higher-privilege function is accessed;
	  ○ Time-based, to shorten the lifetime of any hijacked session.

https://nvd.nist.gov/800-53/Rev4/control/IA-11	

3.2.45 IR-2 – Incident Response Training

Train the organization's personnel for incident response.

1	Same as for "2"

2	• Provide users incident response training and require them to follow it:
	  ○ Consistent with assigned roles and responsibilities (e.g. simpler for regular users, sophisticated for incident responders);
	  ○ Within a predefined time after assuming their role;
	  ○ Afterwards, when the system changes warrant it or with a predefined frequency, whichever occurs first.

3	Same as for "2", plus: • Use simulated events in the training. • Use automated training environments.
https://nvd.nist.gov/800-53/Rev4/control/IR-2	

3.2.46 IR-3 – Incident Response Testing

Ensure that incident response is effective by testing it.

1	Not required
2	Same as for "3"

3	• Carry out tests for validating the effectiveness of the incident response, e.g. using checklists, walk-throughs, table-top exercises, simulations etc. • Include in the testing a determination of the effects of the incidents on operations (e.g. reduction in capabilities), assets and individuals. • Coordinate the testing of the incident response with related plans, e.g. Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.
https://nvd.nist.gov/800-53/Rev4/control/IR-3	

3.2.47 IR-5 – Incident Monitoring

Track and document security incidents.

1	Same as for "2"

2	• Maintain records about each security incident that reflect their current status and details pertinent to handling, digital forensics and trend study.
	• Use as sources any of the following:
	  ○ Incident reports;
	  ○ Incident response team members;
	  ○ Monitoring;
	  ○ User/administrator reports.

3	Same as for "2", plus: • Automate data collection, tracking and analysis.
https://nvd.nist.gov/800-53/Rev4/control/IR-5	

3.2.48 IR-6 – Incident Reporting

Standardize the reporting related to security incidents.

1	• Require personnel to report suspected security incidents to a well-publicized contact point for organizational incident response. • Report security incidents to the required authorities.
2	Same as for "3"
3	Same as for "1", plus: • Automate aspects of the reporting process.
https://nvd.nist.gov/800-53/Rev4/control/IR-6	

3.2.49 IR-7 – Incident Response Assistance

Support users in responding to (suspected) security incidents.

1	• Provide a resource offering advice and assistance to users (other than incident responders) about reporting and handling incidents, e.g. in the form of help desks, assistance groups, and access to forensics services.
2	Same as for "3"

3	Same as for "1", plus: • Automate this assistance, e.g. by an online FAQ, a scheduler for a forensics service appointment etc.
https://nvd.nist.gov/800-53/Rev4/control/IR-7	

3.2.50 IR-8 – Incident Response Plan

Plan the activities to respond to a security incident.

1	Same as for "2"
2	Same as for "3"

3	• Define the incident response plan, addressing:
	  ○ Implementing the incident response capability;
	  ○ The structure and organization of the response capability;
	  ○ The resources and management support required by the response capability;
	  ○ The metrics for the performance of the response capability;
	  ○ Definition of reportable incidents.
	• Review and update the plan with a predefined frequency.
	• Publish copies of the plan to the people with roles in the plan and also update them about changes.
	• Protect the confidentiality of the incident response plan if it ends up containing information that should have restricted circulation.

https://nvd.nist.gov/800-53/Rev4/control/IR-8	

3.2.51 IR-9 – Information Spillage Response

Handle the inadvertent placement of information on components with an insufficient clearance ("spillage").

1	Same as for "2"
2	Same as for "3"
3	• Identify the information involved in the spillage. • Alert predefined personnel / roles of the spill. • Isolate the affected components to contain the spillage. • Eradicate the spilled information from the system components to which it spilled. • Investigate whether the spill involved additional components, and extend the response to those components, too.
https://nvd.nist.gov/800-53/Rev4/control/IR-9	

3.2.52 IR-10 – Integrated Information Security Analysis Team

Have a team capable of incident response.

1	Not required
2	Not required

3	• Establish a multidisciplinary team with competences in all stages of incident response, from threat hunting to the restoration of the service, consisting, e.g. of:
	  ○ Forensic/malicious code analysts;
	  ○ Developers/implementers and tool developers;
	• Real-time operations personnel.

https://nvd.nist.gov/800-53/Rev4/control/IR-10	

3.2.53 MA-2 – Controlled Maintenance

Maintain control over system maintenance activities.	
1	Same as for "2"

2	• Organize maintenance activities in accordance with manufacturer specifications.
	• Approve and monitor all maintenance activities.
	• For off-site maintenance:
	  ○ Require explicit approval for removing equipment from organizational facilities.
	  ○ Sanitize equipment before removing it, to prevent information leaks.
	  ○ Sanitize equipment before reinserting it in the system, to prevent malicious code.
	• Check that security control are still functioning after maintenance of equipment.
	• Update organizational maintenance records, e.g. with:
	  ○ Date and time of maintenance;
	  ○ Maintenance team names and, if applicable, name of internal escort;
	  ○ Maintenance description;
	  ○ Equipment/components replaced or removed.

3	Same as for "2", plus: • Automate the organization of maintenance activities: scheduling, documentation, even performance of the maintenance, as well as the querying of maintenance-related information.
https://nvd.nist.gov/800-53/Rev4/control/MA-2	

3.2.54 MA-3 – Maintenance Tools

Control the tools used during maintenance.	
1	Not required

2	• Approve, control and monitor the tools to be used during maintenance activities (e.g. diagnostic and repair tools).
	• Prior and after maintenance activities inspect maintenance tools and associated storage media for the items below. If the inspection fails, follow incident response procedures:
	  ○ Integrity, to prevent unauthorized and potentially malicious modifications;
	  ○ The absence of malicious code that could infect components of the system;
	  ○ The absence of confidential information being smuggled out of the system.

3	Same as for "2", plus: • Restrict the use of maintenance tools to authorized personnel only.
https://nvd.nist.gov/800-53/Rev4/control/MA-3	

3.2.55 MA-4 – Nonlocal Maintenance

"Remote Maintenance Control"

Maintain control over maintenance performed with nonlocal tools.	
1	• Require nonlocal maintenance activities to be approved prior to carrying them out. ○ Approve only uses consistent with existing policies. • Require nonlocal tools to use strong authenticators prior to establishing a remote maintenance session. • Monitor and maintain an audit trail for monitoring activities with nonlocal tools. • Terminate remote maintenance sessions once the maintenance activities have completed.
2	Same as for "1", plus: • Document nonlocal maintenance activities in the system's Security Plan.

3	Same as for "2", plus:
	• Preserve the protections for the system information by choosing one of the options below:
	  ○ Require the nonlocal information system hosting the maintenance tools to have a comparable information security capability to that of the component being serviced.
	  ○ Remove the component to be serviced from the system, sanitize it against information leakage before servicing it, sanitize it against malicious code after servicing it and before reinserting it into the system.

https://nvd.nist.gov/800-53/Rev4/control/MA-4	

3.2.56 MA-5 – Maintenance Personnel

Limit the security risk from maintenance personnel.	
1	Same as for "2"

2	• Establish a process for authorizing maintenance personnel.
	• Maintain a list of authorized maintenance organizations and personnel.
	• Ensure the required access for maintenance personnel by one of the following two means:
	  ○ Provide maintenance personnel the required access authorizations, persistent or temporary.
	  ○ Designate organization personnel with the required access authorization and technical competence to be the escort and supervisor for the maintenance personnel.

3	Same as for "2", plus:
	• If the maintenance personnel does not have the required clearance to learn the information present on the equipment which requires maintenance:
	  ○ Escort and supervise the maintenance personnel by organization personnel with the appropriate clearance.
	  ○ Remove the component to be serviced from the system, sanitize it against information leakage before servicing it, sanitize it against malicious code after servicing it and before reinserting it into the system. If this is not possible, provide equivalent alternative safeguards.

https://nvd.nist.gov/800-53/Rev4/control/MA-5	

3.2.57 MP-3 – Media Marking

Visually indicate on information media the security needs of the contained information.	
1	Not required
2	Same as for "3"

3	• Apply standardized, human-readable visual marks to information media indicating the data classification label, distribution limitations and any caveats. • Define the types of media which can be exempt from media marking as long as they remain within predefined controlled areas.
https://nvd.nist.gov/800-53/Rev4/control/MP-3	

3.2.58 MP-4 – Media Storage

"Media At Rest Security"	
Protect media appropriately during its storage.	
1	Not required
2	Same as for "3"
3	• Define physical controls and designated controlled areas for storing predefined types of media. • Protects the media with the controls defined above until its destruction or sanitization.
https://nvd.nist.gov/800-53/Rev4/control/MP-4	

3.2.59 MP-5 – Media Transport

"Media In Transit Security"	
Protect system media appropriately during its transport outside controlled areas.	
1	Not required
2	Same as for "3"
3	• Define and apply controls for protecting media (both portable storage media and mobile devices with storage capability) appropriately during transport. • Maintain accountability (chain of custody) for media during transport. • Document media transport activities. • Require personnel involved in the transport of media to be authorized. • Use cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport.
https://nvd.nist.gov/800-53/Rev4/control/MP-5	

3.2.60 MP-8 – Media Downgrading

Lower the security category or classification level of information present on media.	
1	Same as for "2"
2	Same as for "3"

3	• Define processes that remove or obscure information above a given security category or classification level from media, with:
	  ○ The threshold level consistent with the clearance or access authorization of potential recipients.
	  ○ The strength of the downgrading mechanism should ensure that the removed or obscured information cannot be retrieved or reconstructed.
	• Identify the media requiring downgrading if transmitted outside the organization.
	• Apply the downgrading process to the identified media.

https://nvd.nist.gov/800-53/Rev4/control/MP-8	

3.2.61 PE-2 – Physical Access Authorizations

Control which set of individuals has physical access to the facilities where the system resides.

1	Same as for "2"
2	Same as for "3"

3	• Develop and approve a list of individuals authorized to access the facilities.
	  ○ Add individuals as needed.
	  ○ Remove individuals when they should not have access anymore.
	• Review and update the list periodically.
	• Ensure that authorized individuals have access credentials to the facilities as long as they are authorized.

https://nvd.nist.gov/800-53/Rev4/control/PE-2

3.2.62 PE-6 – Monitoring Physical Access

Keep physical access to the system under observation.

1	• Monitor physical access to the facilities housing the system and:
	  ○ Use the observations to detect physical security incidents and launch incident response on the fly.
	  ○ Record physical access events in an access log to support detection of physical incidents through log review and to support after-the-fact investigations.

2	Same as for "1", plus: • Monitor physical intrusion alarms and surveillance equipment.
3	Same as for "2", plus: • For facilities housing other systems, too, perform the monitoring at the level of the information system equipment, not only at the level of the facilities.

https://nvd.nist.gov/800-53/Rev4/control/PE-6

3.2.63 PE-8 – Visitor Access Records

Keep track of visitors (non-organization personnel).

1	Same as for "2"
2	• Maintain and review visitor access logs to the facilities where the system is housed.
3	Same as for "2", plus: • Automate the maintenance and review of the visitor logs.

https://nvd.nist.gov/800-53/Rev4/control/PE-8

3.2.64 PE-10 – Emergency Shutoff

Provide the capability to shut off the system quickly and completely if needed.

1	Not required
2	Same as for "3"

3	• Install an emergency shutoff capability in one or more locations where it can be safely accessed by personnel in case of emergency and protect it from unauthorized activation.
https://nvd.nist.gov/800-53/Rev4/control/PE-10	

3.2.65 PE-11 – Emergency Power

Handle gracefully the loss or failure of the primary power source.

1	Not required

2	• Provide a short-term uninterruptible power supply unit to allow one of the following options:
	  ○ An orderly shutdown of the system;
	  ○ Continued operation of the system until the alternate power supply is activated.

3	Same as for "2", plus: • Provide a long-term alternate power source sufficient for the system to maintain a predefined minimal operational capability.
https://nvd.nist.gov/800-53/Rev4/control/PE-11	

3.2.66 PE-12 – Emergency Lighting

Foresee sufficient lighting for facility evacuation in case of emergency.

1	Same as for "2"
2	Same as for "3"

3	• Employ and maintain emergency lighting for the facilities housing the system such that:
	  ○ It activates automatically in case the primary lighting is lost or fails due to, e.g., power outage or disruption;
	  ○ It covers emergency exits and evacuation routes.

https://nvd.nist.gov/800-53/Rev4/control/PE-12	

3.2.67 PE-16 – Delivery And Removal

Control access to facilities for delivery and removal of system components.

1	Same as for "2"
2	Same as for "3"
3	• Require the delivery and removal of system components from the facility housing the system to be authorized. • Monitor and control entering and exiting the facility for the purpose of delivery or removal of components, if necessary creating a loading/unloading area isolated from the system. • Maintain records of the abovementioned movements.
https://nvd.nist.gov/800-53/Rev4/control/PE-16	

3.2.68 PL-4 – Rules Of Behavior

Enforce secure personnel behaviour.

1	• Define the rules of behaviour that describe the personnel's responsibilities and expected

	behaviour with regard to the system and its information. • Communicate these rules to the personnel. • Obtain a signed acknowledgement ("read, understood and agree to abide by the rules") from personnel before authorizing access to the system and its information. • Review and update the rules of behaviour with predefined frequency and require new signed acknowledgements when the rule set changes.
2	Same as for "3"
3	Same as for "1", plus: • Handle in the rules the appropriate use of social media and public websites with regards to organisational information.
https://nvd.nist.gov/800-53/Rev4/control/PL-4	

3.2.69 PL-7 – Security Concept Of Operations

Make explicit the way to operate the system from the perspective of information security.

1	Same as for "2"
2	Same as for "3"
3	• Define and document a CONOPS (Concept of Operations) containing at a minimum how the organization intends to operate the system from the perspective of information security. • Review and update the Security CONOPS with a predefined frequency and propagate updates into the appropriate organizational documents, e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents.
https://nvd.nist.gov/800-53/Rev4/control/PL-7	

3.2.70 PL-8 – Information Security Architecture

Make the overall approach to information security explicit.

1	Not required
2	Same as for "3"

3	• Develop the information system architecture, describing:
	  ○ Philosophy, requirements, approach, assumptions etc.;
	  ○ Integration with the enterprise architecture;
	  ○ External services.
	• Review and update the architecture with a predefined frequency.
	• Propagate updates to the information security architecture into other documents where they need to be reflected (e.g. Security Plan, PL-7 – Security Concept Of Operations, procurement procedures etc.)

https://nvd.nist.gov/800-53/Rev4/control/PL-8	

3.2.71 PL-9 – Central Management

Centralize the management of security controls and related processes.

1	Same as for "2"
2	Same as for "3"

3	• Centralize the planning, implementation, assessment, authorization and monitoring of security measures.
https://nvd.nist.gov/800-53/Rev4/control/PL-9	

3.2.72 PS-5 – Personnel Transfer

Ensure that individuals departing a role do not continue to have unintended access rights they are not entitled to anymore.

1	Same as for "2"
2	Same as for "3"

3	• When an individual is transferred away from a role, but stays a member of the organization:
	  ○ Rand update their logical and physical access authorizations within a predefined time from the formal transfer.
	  ○ Notify predefined individuals or roles within a predefined time.

https://nvd.nist.gov/800-53/Rev4/control/PS-5	

3.2.73 PS-8 – Personnel Sanctions

Have a formal sanctions process.

1	Same as for "2"
2	Same as for "3"
3	• Employ a formal sanctions process for failure to comply with information security policies and procedures. • Notify the predefined individuals or roles within a predefined time that the sanctions process was initiated, specifying at least the sanctioned individual and the reason.
https://nvd.nist.gov/800-53/Rev4/control/PS-8	

3.2.74 RA-2 – Security Categorization

Use the organizational data classification system.

1	Same as for "2"
2	Same as for "3"
3	• Decide the security categorization / data classification for the system and the information it works with, document it and have it approved by the authorizing official.
https://nvd.nist.gov/800-53/Rev4/control/RA-2	

3.2.75 RA-3 – Risk Assessment

Record and characterize the security risks affecting the object of the assessment.

Supporting and Corporate Measures	
• RA-2 – Security Categorization	

1	• Assess the security risks to which the object of the assessment is exposed. The object of the assessment can be:
	  ○ An information system;
	  ○ A business/mission process;
	  ○ The organization.
	• Record the findings in a document, e.g. in a risk assessment report or as part of a security plan.
	• Disseminate the document among stakeholders with a need-to-know, e.g. the System Owner, the security roles related to the system, developers, administrators etc.
	• Review and update the risk assessment periodically, with a minimum frequency decided by the organization or sooner, if warranted, such as when:
	  ○ There are significant changes to the system;
	  ○ There are significant changes to the environment;
	  ○ Other conditions are met which impact the system's security state.

2	Not used
3	Not used
https://nvd.nist.gov/800-53/Rev4/control/RA-3	

3.2.76 SA-2 – Allocation Of Resources

Ensure the availability of the resources needed by the chosen security measures.	
1	Same as for "2"
2	Same as for "3"
3	• Determine the resource requirements for the security measures. • Include these requirements in mission/business planning, capital planning and investment control process. • Establish a discrete line item in the budget for information security.
https://nvd.nist.gov/800-53/Rev4/control/SA-2	

3.2.77 SA-5 – Information System Documentation

"Security Documentation"	
Ensure that the technical documentation of the system covers information security.	
1	Same as for "2"
2	Same as for "3"

3	• Produce or obtain from suppliers administrator documentation that covers:
	  ○ Secure installation, configuration and operation of the system (e.g. system hardening);
	  ○ Use and maintenance of any security functionality of the system (e.g. cryptographic key / certificate renewal);
	  ○ Any known vulnerabilities of the system.
	• Produce or obtain from suppliers user documentation that covers:
	  ○ Secure usage of the system;
	  ○ The use of user-accessible security functionality;
	  ○ User responsibilities in maintaining security.
	• If security documentation is not obtained from suppliers, document the efforts to obtain it.
	• Disseminate the security documentation to the individuals who need it.
	• Protect the security documentation according to its level of sensitivity.

https://nvd.nist.gov/800-53/Rev4/control/SA-5	

3.2.78 SA-10 – Developer Configuration Management

"Version Control", "Revision Control"	
Take advantage of the benefits of version control.	
1	Not required
2	Same as for "3"
3	• Require the developers to use a configuration management / version control system. • Set up processes that ensure there is change control for the artefacts contributed by the developers (e.g. documentation of the change, review of the change, approval of the change, documentation of the approval). • Track the changes that resolve security flaws and report progress to predefined individuals and roles.
https://nvd.nist.gov/800-53/Rev4/control/SA-10	

3.2.79 SA-11 – Developer Security Testing And Evaluation

"Left Shifted Testing"	
Perform security tests as early as possible.	
1	Not required
2	Same as for "2"
3	• Require the developers to also create and implement a security testing plan, involving, e.g., unit testing, integration testing, system testing, regression testing. • Execute the security testing plan and produce evidence of its execution. • Implement a verifiable flaw remediation process.
https://nvd.nist.gov/800-53/Rev4/control/SA-11	

3.2.80 SA-13 – Trustworthiness

Make explicit the system's trustworthiness (the degree to which it can be expected to preserve the confidentiality, integrity and availability needed by the primary assets).	
1	Not required
2	Same as for "3"

3	• Describe the trustworthiness of the system. • Implement an assurance overlay to achieve the described trustworthiness.
https://nvd.nist.gov/800-53/Rev4/control/SA-13	

3.2.81 SA-14 – Criticality Analysis

Identify critical components and functions of the system (with the worst consequences if they fail to protect security).	
1	Same as for "2"
2	Same as for "3"
3	• Identify core organizational missions supported by the system. • Identify the components essential in supporting those missions or most capable of jeopardizing them.
https://nvd.nist.gov/800-53/Rev4/control/SA-14	

3.2.82 SA-15 – Development Process, Standards, And Tools

Standardize development to satisfy security needs.	
1	Not required
2	Same as for "3"
3	• Define (or require the supplier to use) development processes, standards, tools and tool configurations which address the system's security requirements. • Review the above with predefined frequency and update them if needed.
https://nvd.nist.gov/800-53/Rev4/control/SA-15	

3.2.83 SA-16 – Developer-Provided Training

Accompany the system with training about its security features.	
1	Not required
2	Same as for "3"
3	• Require the delivery of the system to be accompanied by the delivery of a training capability covering the correct use and operation of the implemented security functions, controls, and/or mechanisms.
https://nvd.nist.gov/800-53/Rev4/control/SA-16	

3.2.84 SA-17 – Developer Security Architecture And Design

Accompany the system with documentation about design specifications and security architecture.	
1	Not required
2	Same as for "3"

3	• Require the delivery of the system to be accompanied by the delivery of system documentation on the security design and architecture which is accurate, complete and shows the integration of the system's security architecture in the enterprise security architecture.
https://nvd.nist.gov/800-53/Rev4/control/SA-17	

3.2.85 SA-19 – Component Authenticity

"Anti-Counterfeiting Measures"

Prevent counterfeit components[11] from being incorporated into the system.

1	Same as for "2"
2	Same as for "3"
3	• Define an anti-counterfeit policy. • Report counterfeit components to the appropriate internal and external contact points (e.g. the source of the component, law enforcement etc.).
https://nvd.nist.gov/800-53/Rev4/control/SA-19	

3.2.86 SA-20 – Customized Development Of Critical Components

Ensure that critical components[12] were developed by a trusted entity.

1	Same as for "2"
2	Same as for "3"
3	• If the original developer of a component is not trusted and there are no viable security controls to mitigate that risk, redevelop the component in-house or by a trusted supplier.
https://nvd.nist.gov/800-53/Rev4/control/SA-20	

3.2.87 SA-21 – Developer Screening

Perform personnel screening for developers.

1	Same as for "2"
2	Same as for "3"
3	• Define screening criteria for developers (e.g. required governmental assigned access authorizations, additional criteria defined by the organization). • Require individuals to pass the screening before they are assigned as developers of the system.
https://nvd.nist.gov/800-53/Rev4/control/SA-21	

3.2.88 SA-22 – Unsupported System Components

Handle systematically components[13] whose support by their suppliers has ceased.

[11] Components are elements built outside the organization, which participate in the construction of modern systems through composition. This includes both hardware components and software ones (libraries, widgets, themes etc.)

[12] Critical components are components whose malfunction would have markedly more serious consequences than the malfunction of non-critical components.

[13] See definition from footnote on page 96.

1	Same as for "2"
2	Same as for "3"

3	• When support for a component by its supplier ends, implement one of the following options:
	  ○ Replace it with a still-supported equivalent component.
	  ○ Provide justification and obtain approval for its continued use.

https://nvd.nist.gov/800-53/Rev4/control/SA-22	

3.2.89 SC-12 – Cryptographic Key Establishment And Management

Protect cryptographic keys appropriately during their life cycle.

1	Same as for "2"
2	• Define and apply key management procedures in accordance to organizational policies and procedures on the matter and cover: key generation, distribution, storage, access, and destruction. • Manage "trust stores" (repositories of keys and accompanying information) containing the only keys approved to serve as "trust anchors" (trusted implicitly, not because their trustworthiness can be established using other trusted keys).
3	Same as for "2", plus: • Ensure that the availability of the system is maintained even in the event of loss of cryptographic keys by the users.
https://nvd.nist.gov/800-53/Rev4/control/SC-12	

3.2.90 SC-15 – Collaborative Computing Devices

Prevent collaboration devices from being used for spying.

1	Same as for "2"
2	Same as for "3"

3	• Prevent spying through collaborative devices (e.g. teleconferencing cameras and microphones, webcams etc.) by one or both of the following:
	  ○ Prohibiting their remote activation;
	  ○ Signalling their activation to the users physically present.

https://nvd.nist.gov/800-53/Rev4/control/SC-15	

3.2.91 SC-16 – Transmission Of Security Attributes

Transmit the information's security attributes[14] along with the transmitted information.

1	Same as for "2"
2	Same as for "3"
3	• Define which security attributes to transmit along with each type of information when it is transmitted between systems or between components of the system.
https://nvd.nist.gov/800-53/Rev4/control/SC-16	

[14] Security attributes are metadata with a role in security, e.g. data owner, modification time, classification label, origin, virus checked or not etc.

3.2.92 SC-17 – Public Key Infrastructure Certificates

Specify how Public Key Infrastructure ("PKI") certificates are used in the system.

1	Not required
2	Same as for "3"
3	• Define a policy for issuing certificates and follow it when issuing them. • Maintain a list of service providers approved to act as PKI certificate suppliers.

https://nvd.nist.gov/800-53/Rev4/control/SC-17

3.2.93 SC-20 – Secure Name / Address Resolution Service (Authoritative Source)

Be a trustworthy name / address resolution service.

1	Same as for "2"
2	Same as for "3"
3	• Alongside responses to external name/address resolution queries, provide artefacts allowing authentication of the data origin and verification of the integrity of the responses. • Provide security information about DNS child zones (their security status, chain of trust between parent and child domains etc.)

https://nvd.nist.gov/800-53/Rev4/control/SC-20

3.2.94 SC-21 – Secure Name / Address Resolution Service (Recursive Or Caching Resolver)

Perform due diligence as a client of a name / address resolution service.

1	Same as for "2"
2	Same as for "3"
3	• Request from the resolution service the necessary artefacts for data origin authentication and data integrity verification and only use the response if it passes the authentication and verification.

https://nvd.nist.gov/800-53/Rev4/control/SC-21

3.2.95 SC-22 – Architecture And Provisioning For Name / Address Resolution Service

Observe secure engineering principles in the design of the name / address resolution service.

1	Same as for "2"
2	Same as for "3"
3	• Ensure that the resolution service is fault-tolerant (e.g. through redundancy among its components). • Ensure that the resolution service available to internal systems is separate from that available to external systems.

https://nvd.nist.gov/800-53/Rev4/control/SC-22

3.2.96 SC-24 – Fail In Known State

Know the characteristics of the state of a failed system.

1	Not required
2	Not required
3	• Establish a catalogue relating failure types to states the system is in when it fails in that type (including what system information it preserves). • Build the system to fail according to the catalogue.

https://nvd.nist.gov/800-53/Rev4/control/SC-24

3.2.97 SC-25 – Thin Nodes

"Network Computing"

Reduce the attack surface by using components with minimal functionality and storage.

1	Same as for "2"
2	Same as for "3"
3	• Use computing nodes that store minimal information and perform minimal processing locally, relying on network storage and server-side processing.

https://nvd.nist.gov/800-53/Rev4/control/SC-25

3.2.98 SC-26 – Honeypots

Provide fake targets for attack.

1	Not required
2	Same as for "2"

3	• Deploy components destined to be attacked by unwitting attackers:
	  ○ Mimic real components.
	  ○ Do not store real information or interact with real components.
	  ○ Instrument them for detection, recording and recovery of attacker activity.

https://nvd.nist.gov/800-53/Rev4/control/SC-26

3.2.99 SC-27 – Platform-Independent Applications

Increase availability by choosing applications that run on multiple platforms.

1	Same as for "2"
2	Same as for "3"

3	• Choose applications that run on multiple:
	  ○ Computer architectures;
	  ○ Operating systems;
	  ○ Implementations of middleware (e.g. Java application servers)

https://nvd.nist.gov/800-53/Rev4/control/SC-27

3.2.100 SC-29 – Heterogeneity

"Monoculture Avoidance"

Prevent all components failing in the same way by implementing them in a variety of technologies.

1	Same as for "2"
2	Same as for "3"
3	• Employ a diverse set of technologies for components with the same function (e.g. database, web server, operating system).

https://nvd.nist.gov/800-53/Rev4/control/SC-29

3.2.101 SC-30 – Concealment And Misdirection

"Deception Technologies"

Confuse, mislead and delay adversaries by using deception.

1	Not required
2	Not required
3	• Employ concealment and misdirection techniques (e.g. fake error messages, fake product names and version numbers) to confuse, mislead and delay adversaries.

https://nvd.nist.gov/800-53/Rev4/control/SC-30

3.2.102 SC-32 – Information System Partitioning

Provide defense in depth by having different components reside in different physical domains or environments.

1	Not required
2	Same as for "3"
3	• Split the system into partitions and distribute the partitions onto different physical domains or environments (e.g. based on their security categories) to reduce the likelihood of an attack spreading between partitions. • Control the interfaces between the partitions to allow only legitimate transmissions and monitor them for illegitimate transmission attempts.

https://nvd.nist.gov/800-53/Rev4/control/SC-32

3.2.103 SC-35 – Honeyclients

Detect online sources of malicious code by employing fake client components.

1	Not required
2	Not required

3	• Deploy components which mimic legitimate client components and:
	  ○ Proactively probe the internet for predefined types of information services (e.g. web servers, file sharing services, DNS responders, time services etc.).
	  ○ Analyze the responses / resources returned for malicious elements (e.g. counterfeit web site certificates, malware-infected files, malformed responses for triggering a buffer overflow etc.).
	  ○ Are hardened and isolated from the real components to prevent real infection.

https://nvd.nist.gov/800-53/Rev4/control/SC-35	

3.2.104 SC-36 – Distributed Processing And Storage

Achieve resilience by distributing processing and storage functions across physical locations.	
1	Same as for "2"
2	Same as for "3"
3	• Split the components of the system into potentially overlapping subsets and have each subset reside in a different physical location.
https://nvd.nist.gov/800-53/Rev4/control/SC-36	

3.2.105 SC-37 – Out-Of-Band Channels

Raise the bar for an adversary by having a second, separate communication channel available.	
1	Same as for "2"
2	Same as for "3"
3	• Foresee a second transport / transmission channel that would be left intact by an attack on the primary channel, to be used in the recovery and reconstruction of the primary channel (e.g. transport of data on removable storage media when the network is down).
https://nvd.nist.gov/800-53/Rev4/control/SC-37	

3.2.106 SC-38 – Operations Security

"OpSec"	
Apply risk management to the operational aspects[15] of the organization and system.	
1	Not required
2	Same as for "3"
3	• Employ a systematic process (of risk management) for implementing safeguards that avoid security mistakes and deny adversaries information that could aid them in an attack, e.g., user identities, suppliers, processes, requirements, specifications, known risks and vulnerabilities, security measure implementation details etc.
https://nvd.nist.gov/800-53/Rev4/control/SC-38	

[15] In addition to protecting the information system itself against risks, this Measure aims to deprive adversaries of any help the organisation that builds or operates the system might inadvertently give them. For example, by keeping the identities of the individuals with privileged access from becoming public, those individuals are somewhat protected against attempts to bribe or blackmail them. By taking a different route every time, the vehicle in which the data back-up media are transported to the storage location is more protected against robbery attempts.

3.2.107 SC-41 – Port And I/O Device Access

Reduce the attack surface by eliminating unneeded ports and I/O devices.	
1	Same as for "2"
2	Same as for "3"
3	• Physically disable, remove or block input/output channels present by default on equipment, but not needed by the system, e.g. USB or Firewire ports, optical drives etc.
https://nvd.nist.gov/800-53/Rev4/control/SC-41	

3.2.108 SC-42 – Sensor Capability And Data

Prevent environmental sensors from being used for spying.	
1	Same as for "2"
2	Same as for "3"

3	• When devices have environmental sensors (e.g. mobile devices having GPS/location sensors, accelerometers, cameras, microphones) do one or both of the following:
	  ○ Prohibit their remote activation;
	  ○ Signal their activation to the users.

https://nvd.nist.gov/800-53/Rev4/control/SC-42	

3.2.109 SC-43 – Usage Restrictions

Restrict the use of components that could pose risks[16] if used maliciously to limit the possible damage.	
1	Same as for "2"
2	Same as for "3"
3	• Establish usage restrictions and implementation guidance for predefined components. • Authorize, monitor and control the use of such components.
https://nvd.nist.gov/800-53/Rev4/control/SC-43	

3.2.110 SC-44 – Detonation Chambers

"Dynamic Execution Environments"	
Allow malicious code to execute for analysis purposes in environments isolated from the system.	
1	Not required
2	Not required

[16] Example risky component: the microphone of a public announcement system, which could be misused to cause panic in a building.

3	• Employ a "detonation chamber" capability in the analysis of malicious code, an environment with the following characteristics: ○ Supports for a short term the execution of malicious code (e.g. from malware or malicious code in a web page); ○ Is protected and isolated from the rest of the IT environment to prevent the malicious code from "breaking out". ○ Is destroyed at the end of the analysis.
https://nvd.nist.gov/800-53/Rev4/control/SC-44	

3.2.111 SI-6 – Security Function Verification

Ensure that the system's security functions are operational.

1	Not required
2	Not required
3	• Verify the correct operation of the system's security functions with a predefined frequency and respond in predefined ways when anomalies are detected, e.g. notifying a predefined individual or role, shut down or restart the system etc.
https://nvd.nist.gov/800-53/Rev4/control/SI-6	

3.2.112 SI-8 – Spam Protection

Protect the users from unsolicited messages.

1	Not required
2	Same as for "3"
3	• Employ spam protection mechanisms to detect and handle appropriately unsolicited messages at the system's entry points to prevent incoming spam and at the exit points to prevent internally-generated spam. • Enable the auto-update feature of the spam protection mechanisms. • Manage the spam protection centrally, for better coordination.
https://nvd.nist.gov/800-53/Rev4/control/SI-8	

3.2.113 SI-10 – Information Input Validation

Ensure that the system accepts only inputs it is designed to process.

1	Not required
2	Same as for "3"
3	• Test whether input values have the intended syntax and semantics for that input (e.g. numeric/alphanumeric/date type, character set, numeric range etc.). • Reject the input, do not process it, if it fails validation.
https://nvd.nist.gov/800-53/Rev4/control/SI-10	

3.2.114 SI-11 – Error Handling

"Error Messages"

Ensure that error messages are helpful for troubleshooting, but not to an adversary.

1	Not required
2	Same as for "3"

3	• Configure the content of error messages displayed by the system when it cannot recover from an error to be:
	  ○ Helpful for determining the appropriate corrective actions.
	  ○ Unhelpful for targeting an attack.
	• Configure the recipients of error messages to include only predefined individuals and roles.

https://nvd.nist.gov/800-53/Rev4/control/SI-11	

3.2.115 SI-12 – Information Handling And Retention

Manage the life cycle of the information contained in the system and provided as an output.

1	Same as for "2"
2	Same as for "3"

3	• Define the appropriate ways to handle information contained in or obtained from the system, to ensure that the organization and system are compliant with all the relevant regulations.
	• Define what happens to information when it is not needed anymore:
	  ○ What external entities it is sent to for historic archival (e.g. museums);
	  ○ The duration after which the information is disposed.

https://nvd.nist.gov/800-53/Rev4/control/SI-12	

3.2.116 SI-13 – Predictable Failure Prevention

Replace components which wear out before they fail.

1	Not required
2	Same as for "3"
3	• Determine the mean time to failure (MTTF) for components for which it can be predicted. • Derive from the MTTF a time threshold at which the likelihood that the component has failed is balanced out by the waste of replacing the component prematurely. • Schedule the replacement of the component when its time threshold has been reached.
https://nvd.nist.gov/800-53/Rev4/control/SI-13	

3.2.117 SI-15 – Information Output Filtering

Detect attacks based on how they alter the output of system components.

1	Same as for "2"
2	Same as for "3"
3	• Test the output of components/programs/applications for deviations from the expected characteristics (e.g. length, structure, content etc.) which could indicate attack attempts. • Respond to failed tests by blocking the output, signalling an error to any components expecting that output and triggering predefined alerting procedures.
https://nvd.nist.gov/800-53/Rev4/control/SI-15	

3.2.118 SI-16 – Memory Protection	
"Executable-Space Protection"	
Prevent memory areas used for storing data from being interpreted as storing code.	
1	Not required
2	Same as for "3"
3	• Define and implement safeguards to prevent unintended execution of memory areas containing data, which is a powerful avenue of attack for adversaries.
https://nvd.nist.gov/800-53/Rev4/control/SI-16	

3.2.119 SI-17 – Fail-Safe Procedures	
"Error Handling For Humans"	
Manage the response to predefined failure conditions.	
1	Same as for "2"
2	Same as for "3"
3	• For anticipated failures of the system that require human response, too, design a catalogue mapping failure conditions to response actions by personnel (e.g. do nothing, restart component, trigger incident response etc.)
https://nvd.nist.gov/800-53/Rev4/control/SI-17	

3.3 Corporate Measures

3.3.1 AC-1 – Access Control Policy And Procedures	
Document the approach to access control.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to access control, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the access control policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/AC-1	

3.3.2 AT-1 – Security Awareness And Training Policy And Procedures	
Document the approach to security awareness and training.	
1	Same as for "2"
2	Same as for "3"

3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to security awareness and training, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the security awareness and training policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/AT-1	

3.3.3 AU-1 – Audit And Accountability Policy And Procedures

Document the approach to audit and accountability.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to audit and accountability, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the audit and accountability policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/AU-1	

3.3.4 CA-1 – Security Assessment And Authorization Policy And Procedures

Document the approach to security assessment[17] and authorization[18].	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to security assessment and authorization, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the security assessment and authorization policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/CA-1	

3.3.5 CM-1 – Configuration Management Policy And Procedures

Document the approach to configuration management[19].	
1	Same as for "2"
2	Same as for "3"

[17] See CA-2 – Security Assessments
[18] See CA-6 – Security Authorization
[19] Configuration Management is the ensemble of activities described in the other CM-* measures, whose purpose is to ensure that the organization maintains knowledge and control over the effective values of the configurable parameters of the system during operation.

3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to configuration management, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the configuration management policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/CM-1	

3.3.6 CM-8 – Information System Component Inventory

Know at all times the composition of the system in terms of components in its scope and their characteristics necessary for tracking and reporting.

Supporting and Corporate Measures

None

1	• Keep an inventory of the components of the system, which:
	  ○ Is current – it accurately reflects the current state;
	  ○ Is complete – it includes all components that are in scope of the system;
	  ○ Is granular – records the details of the component necessary for fulfilling the organization's tracking and reporting needs;
	  ○ Supports effective accountability.
	• The inventory is updated during periodic reviews of the actual state of the System.

2	Same as for "1", plus: • Include "inventory updating" as a step in the procedures for installation/deployment, update and removal/decommissioning of components. • Use automation for detecting unauthorized components and for triggering a reaction to such discoveries (the reaction would be part of another Mitigating Measure). • Avoiding having multiple entries in the component inventory for the same component.
3	Same as for "2", plus: • The inventory is updated in an automated fashion as the system composition evolves. • Have individuals assigned as accountable for each inventory item.
https://nvd.nist.gov/800-53/Rev4/control/CM-8	

3.3.7 CM-9 – Configuration Management Plan

Organize and plan configuration management activities.

1	Not required
2	Same as for "3"

3	• Develop, document and implement the plan for configuration management, covering at least:
	  ○ Configuration management related roles, responsibilities, processes and procedures;
	  ○ A process for discovering configuration items during the development life cycle and putting them under configuration management;
	  ○ How to protect the configuration management plan itself according to its security needs.

https://nvd.nist.gov/800-53/Rev4/control/CM-9	

3.3.8 CP-1 – Contingency Planning Policy And Procedures

Document the approach to contingency planning.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to contingency planning, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the contingency planning policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/CP-1	

3.3.9 IA-1 – Identification And Authentication Policy And Procedures

Document the approach to identification and authentication.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to identification and authentication, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the identification and authentication policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/IA-1	

3.3.10 IR-1 – Incident Response Policy And Procedures

Document the approach to incident response.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to incident response, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the incident response policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/IR-1	

3.3.11 MA-1 – System Maintenance Policy And Procedures

Document the approach to system maintenance.	
1	Same as for "2"
2	Same as for "3"

3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to system maintenance, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the system maintenance policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/MA-1	

3.3.12 MP-1 – Media Protection Policy And Procedures

Document the approach to media protection.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to media protection, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the media protection policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/MP-1	

3.3.13 PE-1 – Physical And Environmental Protection Policy And Procedures

Document the approach to physical and environmental protection.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to physical and environmental protection, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the physical and environmental protection policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/PE-1	

3.3.14 PL-1 – Security Planning Policy And Procedures

Document the approach to security planning[20].	
1	Same as for "2"
2	Same as for "3"

[20] Security Planning is the set of activities for satisfying the security needs of the system (which first need to be determined) through security measures (such as the ones in this catalogue).

3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to security planning, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the security planning policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/PL-1	

3.3.15 PS-1 – Personnel Security Policy And Procedures

Document the approach to personnel security.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to personnel security, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the personnel security policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/PS-1	

3.3.16 RA-1 – Risk Assessment Policy And Procedures

Document the approach to risk assessment.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to risk assessment, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the risk assessment policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/RA-1	

3.3.17 SA-1 – System And Services Acquisition Policy And Procedures

Document the approach to system and services acquisition.	
1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to system and services acquisition, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the system and services acquisition policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/SA-1	

3.3.18 SA-8 – Security Engineering Principles

Use well-known security engineering principles throughout the life cycle of the system.

1	Not required
2	Same as for "3"

3	• Maintain a set of security engineering principles, updated as the technical literature advances, e.g.:
	  ○ Design layered protections / defense in depth;
	  ○ Gather security requirements at the same time as functional requirements;
	  ○ Delineate physical and logical security boundaries;
	  ○ Etc.
	• Apply the security engineering principles in the specification, design, development, implementation, and modification of the system.

https://nvd.nist.gov/800-53/Rev4/control/SA-8

3.3.19 SC-1 – System And Communications Protection Policy And Procedures

Document the approach to system and communications protection.

1	Same as for "2"
2	Same as for "3"
3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to system and communications protection, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the system and communications protection policy and procedures with predefined frequencies.

https://nvd.nist.gov/800-53/Rev4/control/SC-1

3.3.20 SC-19 – Voice Over Internet Protocol

Control the use of VoIP technologies.

1	Not required
2	Same as for "3"
3	• Establish usage restrictions and implementation guidance for VoIP technologies in order to safeguard the system's security. • Require authorization prior to deployment, monitor and control VoIP technologies used within the system.

https://nvd.nist.gov/800-53/Rev4/control/SC-19

3.3.21 SI-1 – System And Information Integrity Policy And Procedures

Document the approach to system and information integrity.

1	Same as for "2"
2	Same as for "3"

3	• Develop and disseminate to the appropriate individuals a policy and procedures describing the organization and high level principles of the approach to system and information integrity, covering at least: purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • Review and update the system and information integrity policy and procedures with predefined frequencies.
https://nvd.nist.gov/800-53/Rev4/control/SI-1	

3.3.22 PM-1 – Information Security Program Plan

A plan geared towards the security of the organization's information, not just of the system.

Supporting and Corporate Measures

None

1	Not used

2	• Develop, periodically review and update a plan which:
	  ○ Identifies the requirements for the security program.
	  ○ Describes the program management controls and common controls to meet those requirements.
	  ○ Identifies and assigns individuals to roles for management commitment, coordination and compliance.
	  ○ Reflects coordination among organizational entities with different responsibilities.
	  ○ Is approved by a senior official with accountability and responsibility for the risk to organizational operations, assets, other organizations etc.
	• Protect the confidentiality and integrity of the plan.

3	Not used
https://nvd.nist.gov/800-53/Rev4/control/PM-1	

3.3.23 PM-2 – Senior Information Security Officer

"Chief Information Security Officer"

Appoint a senior information security officer.

1	Same as for "2"
2	Same as for "3"
3	Designate a senior organization official with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
https://nvd.nist.gov/800-53/Rev4/control/PM-2	

3.3.24 PM-3 – Information Security Resources

Make available the resources needed by Information Security activities.

1	Not required
2	Same as for "3"
3	Include the resources for information security in all capital planning and investment requests, providing a business case and ensure that they are made available as planned.
https://nvd.nist.gov/800-53/Rev4/control/PM-3	

3.3.25 PM-4 – Plan Of Action And Milestones Process

Manage the implementation of the Security Plan.

1	Not required
2	Same as for "3"
3	• Implement a process for developing and maintaining the plan of action, including milestones, for the implementation of the planned Measures from the Security Plan. • Report on the progress of the plan of action and on achieving the milestones according to the organization's practices.

https://nvd.nist.gov/800-53/Rev4/control/PM-4

3.3.26 PM-5 – Information System Inventory

Reflect the real set of system components in a representation that makes it possible to analyse and report on it.

1	Same as for "2"
2	Same as for "3"
3	• Set up and maintain an inventory of the system's components.

https://nvd.nist.gov/800-53/Rev4/control/PM-5

3.3.27 PM-6 – Information Security Measures Of Performance

Have the ability to measure the performance of the security measures deployed for the system.

1	Not required
2	Not required
3	• Establish performance metrics for the security measures of the system. • Monitor the performance metrics and report on them.

https://nvd.nist.gov/800-53/Rev4/control/PM-6

3.3.28 PM-7 – Enterprise Architecture

"Enterprise Security Architecture"

Take information security into account when developing the enterprise architecture.

1	Not required
2	Same as for "3"
3	• Develop a security architecture at a system-of-systems level integrating the security requirements of the individual systems.

https://nvd.nist.gov/800-53/Rev4/control/PM-7

3.3.29 PM-8 – Critical Infrastructure Plan

Plan the protection of key resources and of infrastructure deemed critical[21].	
1	Not required
2	Same as for "3"
3	• Develop a plan for addressing in a priority-based way security issues in the development, documentation, and updating of infrastructure and resources deemed critical or key.
https://nvd.nist.gov/800-53/Rev4/control/PM-8	

3.3.30 PM-9 – Risk Management Strategy

Have a comprehensive strategy for managing risk in the organization.	
1	Not required
2	Same as for "3"
3	• Define, periodically review and update if necessary a risk management strategy covering at least: o An unambiguous expression of the risk tolerance for the organization; o Acceptable risk assessment methodologies; o Acceptable risk mitigation strategies; o A process for consistently evaluating risk across the organization; o Approaches for monitoring risk over time. • Implement the strategy consistently across the organisation
https://nvd.nist.gov/800-53/Rev4/control/PM-9	

3.3.31 PM-10 – Security Authorization Process

Assign individuals to roles and responsibilities through a deliberate process.	
1	Not required
2	• Implement a process for the assignment of roles and responsibilities to individuals, ensuring: o No assignment of roles and responsibilities without approval at the appropriate level; o A deliberation-based decision to approve the assignment of roles and responsibilities to individuals; o Documentation and audit log of the steps of the process.
3	Same as for "2", plus: • Integrate the security authorization process into the organization-wide risk management program, e.g. with the continuous monitoring processes.
https://nvd.nist.gov/800-53/Rev4/control/PM-10	

3.3.32 PM-11 – Mission/Business Process Definition

Ensure that the mission/business processes are defendable[22].

[21] "Key resources" and "critical infrastructure" are labels that help in the prioritization of protection strategies for assets and resources independent of the Business Impact Analysis (BIA) performed as part of a Risk Assessment. The labels may be the only data available when a BIA is not available. The labels may supersede the values obtained through BIA in certain regulatory frameworks. The criteria for assigning these labels are left to "applicable [...] laws, Executive Orders, directives, policies, regulations, standards, and guidance" in the source document.

1	Not required
2	Same as for "3"
3	• Explicitly define the mission/business processes. • Determine the information protection needs arising from the defined mission/business processes and if these needs are deemed impossible to satisfy, revise the processes until the protection is deemed achievable.
https://nvd.nist.gov/800-53/Rev4/control/PM-11	

3.3.33 PM-12 – Insider Threat Program

Address the insider threat in a comprehensive manner.

1	Not required
2	Same as for "3"

3	• Implement a program to address the insider threat, containing at least the following elements:
	  ○ Leadership by a senior organization official;
	  ○ Security measures to detect and prevent malicious insider activity (e.g. monitoring, awareness training, departmental self-assessments of posture, prediction based on HR records etc.);
	• A cross-disciplinary incident handling capability for insider threats as part of the incident handling team.

https://nvd.nist.gov/800-53/Rev4/control/PM-12	

3.3.34 PM-13 – Information Security Workforce

Cultivate the skill set of the personnel involved in information security.

1	Not required
2	Not required

3	• Maintain and improve the skill level of the workforce involved in information security by:
	  ○ Defining the knowledge and skill levels needed by each role in the information security workforce;
	  ○ Developing and maintaining role-based training programs for achieving the needed knowledge and skill levels;
	  ○ Providing standards for measuring knowledge and skill levels to be used in evaluating the effectiveness of the training programmes;
	  ○ Providing career paths in information security.

https://nvd.nist.gov/800-53/Rev4/control/PM-13	

3.3.35 PM-14 – Testing, Training, And Monitoring

[22] When the specified mission/business processes are deemed impossible to secure ("defend") with realistic measures, the processes should be modified to still achieve the business goals, but be possible to secure. E.g. if support requests are foreseen to be sent by email, but it is unfeasible to protect against spam emails, the support process may switch to a web-based platform.

Ensure the execution of security testing[23], training[24] and monitoring[25] plans.	
1	Not required
2	Same as for "3"
3	• Implement a control process to ensure that security testing, training and monitoring plans are developed, maintained, executed in a timely manner, reviewed periodically and updated if necessary.
https://nvd.nist.gov/800-53/Rev4/control/PM-14	

3.3.36 PM-15 – Contacts With Security Groups And Associations

Cultivate the necessary contacts with external organizations within the security community.	
1	Not required
2	Not required

3	• Establish and institutionalize contacts with external organizations within the security community to:
	  ○ Facilitate ongoing education and training for the information security workforce.
	  ○ Maintain currency / be aware of the state of the art information security practices, techniques and technologies.
	  ○ Share current security-related information (e.g. threats, vulnerabilities, incidents etc.)

https://nvd.nist.gov/800-53/Rev4/control/PM-15	

3.3.37 PM-16 – Threat Awareness Program

Raise awareness in the organization about the current threats to it and to the system.	
1	Not required
2	Same as for "2"
3	• Prepare personnel to better protect the system's and organization's security by sharing current security information relevant to their activities (e.g. current attack campains, adversary tactics/techniques/procedures, warnings about threats that are likely to occur etc.). • Prepare the security community to better protect their individual and collective security by sharing bilaterally or multilaterally threat information across organizational boundaries, with the appropriate agreements in place.
https://nvd.nist.gov/800-53/Rev4/control/PM-16	

[23] Security testing includes the activities mentioned in CA-8 – Penetration Testing, RA-5 – Vulnerability Scanning, SA-11 – Developer Security Testing And Evaluation.

[24] See the Measures from the AT-* family.

[25] See SI-4 – Information System Monitoring, CA-7 – Continuous Monitoring, IR-5 – Incident Monitoring and PE-6 – Monitoring Physical Access for monitoring plans.

ANNEX A: REFERENCES AND RELATED DOCUMENTS

ID	Reference or Related Document
[CD46/2017]	COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission
[IR46/2017]	COMMISSION DECISION of 13.12.2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission
[MAGERIT]	MAGERIT versión 3.0. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* *Libro II - Catálogo de Elementos* Madrid, octubre de 2012 Ministerio de Hacienda y Administraciones Públicas Secretaría General Técnica Subdirección General de Información
[EBIOS]	EBIOS version 2 *Expression des Besoins et Identification des Objectifs de Sécurité* *Section 4 – Tools for Assessing ISS Risks* 5 February 2004 Document produced by the DCSSI Advisory Office (SGDN / DCSSI / SDO / BCS) in collaboration with the EBIOS Club Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil
[ENISA]	*Cloud Computing Benefits, risks and recommendations for information security v2.0* Rev.B – December 2012 ENISA – European Network and Information Security Agency
[OWASP]	*Top 10 Cloud Security Risks* OWASP - Open Web Application Security Project
[CSA]	*Top Threats to Cloud Computing* 2016 CSA - Cloud Security Alliance
[NIST]	NIST Special Publication SP800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2015

ANNEX B: ACRONYMS

CONOPS	CONcept of OPerationS
CRAM	Challenge-Response Authentication Mechanism
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FAQ	Frequently Asked Questions
GPS	Global Positioning System
HR	Human Resources
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IPv4	Internet Protocol, version 4
IPv6	Internet Protocol, version 6
IT	Information Technology
ITSRM²	IT Security Risk Management Methodology
MAC address	Media Access Control address
MTTF	Mean Time To Failure
NIST	National Institutde for Standards and Technology
NTP	Network Time Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDL	Security Development Lifecycle
TEMPEST	Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
TLS	Transport Layer Security
TOTP	Time-based One Time Password
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTC	Universal Time Coordinated
VPN	Virtual Private Network
WORM	Write Once, Read Many