Cybersecurity Governance

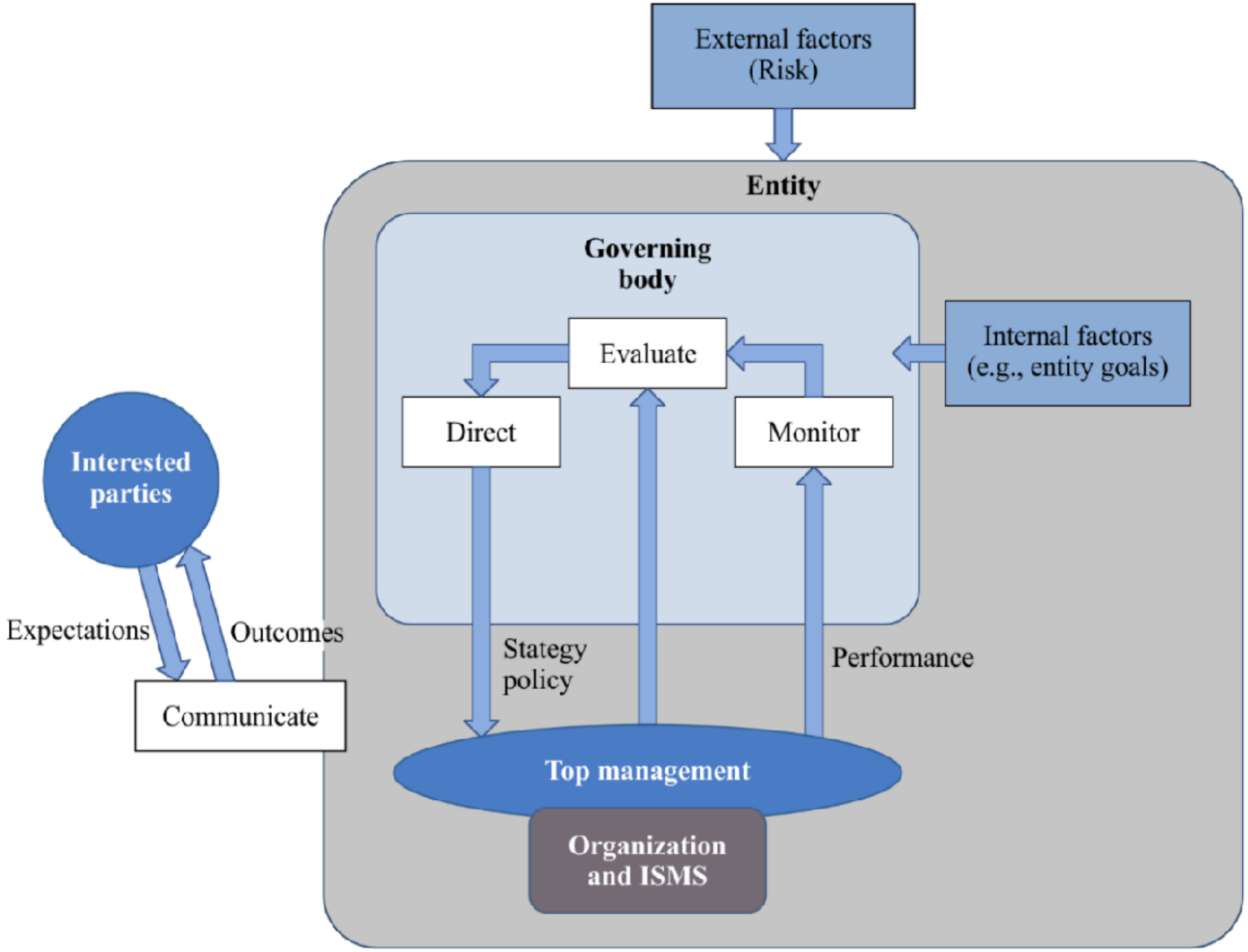
Cybersecurity Governance

- Cybersecurity Governance monitor, evaluate and direct, an organization's information security with the intent to aligning security with business objectives, ensuring accountability, and managing risks effectively.

  Inspired by ISO 27014 – Governance of Information Security

- Several other definitions are possible emphasizing different aspects

Cybersecurity Governance



ISO 27014

ISO 27014 – Information Security Governance

- It formally describes governance processes
- The ***entity*** is the organization whose information security is to be governed
- External Factors (Risk)
  - Threat landscape, regulations, geopolitical risks
  - Influence strategic risk evaluation
  - Provide context for governance decisions
- Internal Factors (Entity Goals)
  - Business objectives and mission
  - Operational constraints and priorities
  - Drive alignment of **ISMS** with organizational strategy

ISMS

In Information Security Management System is defined by ISO27001 as a “management system” consisting of a set of interrelated or interacting elements used to establish, implement, operate, monitor, review, maintain, and improve information security.

Essentially

a **set of policies, procedures, processes, and controls** that an organization implements to **systematically protect its information assets**.

Governing Body

It is the highest authority for information security governance within the entity

- Ensures information security supports business goals
- Responsible for strategic evaluation, direction, and oversight

Top Management

- Implements strategy and policies from the governing body
- Oversees ISMS operations and resource usage
- Reports performance metrics upward

Top management: CEO, CFO, COO, BU directors.. **CIO**, **CISO**, **DPO**,…

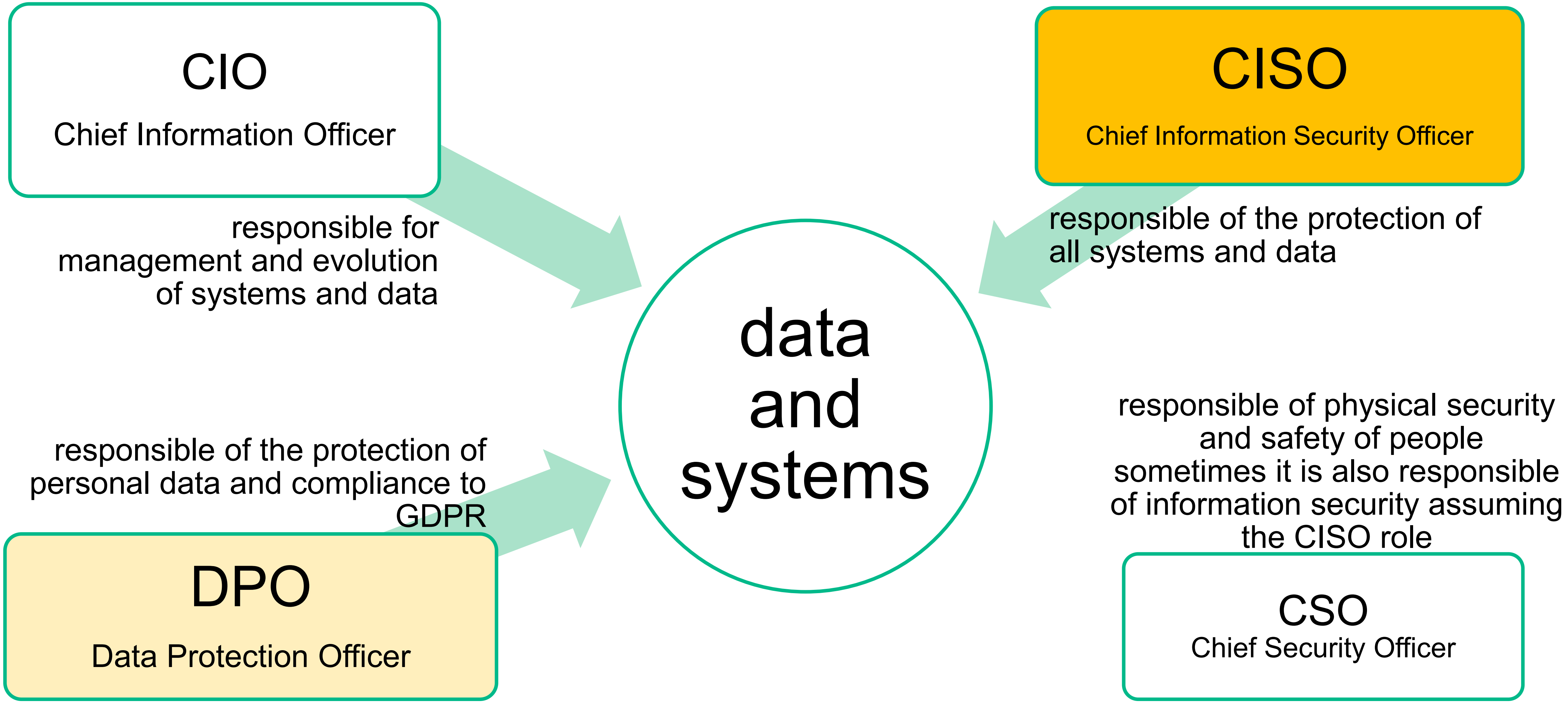
Core governance processes

- **Evaluate.** The governing body…
  - analyzes risks and performance,
  - evaluates internal and external factors,
  - assesses whether the ISMS supports business objectives.
- **Direct.** After evaluation, the governing body…
  - issues directives,
  - sets strategy and security policy,
  - defines risk appetite,
  - allocates resources.
- **Monitor.** The governing body…
  - receives performance information from top management,
  - checks if directives are being followed,
  - reviews audits, incidents, KPIs.

Communication with Interested Parties

- Stakeholders provide expectations (customers, regulators, staff)
- Organization delivers outcomes and transparency
- Ensures continuous alignment and trust

Information security professional profiles



CIO

Chief Information Officer

responsible for management and evolution of systems and data

CISO

Chief Information Security Officer

responsible of the protection of all systems and data

data and systems

responsible of the protection of personal data and compliance to GDPR

DPO

Data Protection Officer

responsible of physical security and safety of people
sometimes it is also responsible of information security assuming the CISO role

CSO
Chief Security Officer

Security Posture

- Security posture is the collective state of an organization’s cybersecurity readiness, that determine how well it can prevent and manage security risks.
- It encompasses…

Component	Description
Policies & Procedures	Documented rules for security, access, data handling, incident response, etc.
Technical Controls	Firewalls, antivirus, intrusion detection, encryption, multi-factor authentication.
Operational Practices	Monitoring, patch management, backups, vulnerability management.
Risk Management	Identification of risks, risk appetite, risk tolerance, and mitigation strategies.
Awareness & Culture	Employee training, security awareness, and adherence to best practices.
Incident Response & Resilience	Capability to detect, respond to, and recover from cyber incidents.
Compliance & Governance	Alignment with regulations, standards, and industry best practices.

CISO and the Security Posture

- The **CISO defines, manages, and improves the cybersecurity posture**.

CISO's work (1)

- Strategy
  - Define cybersecurity strategy aligned with business goals
  - Adopt *governance frameworks* (e.g. ISO 27001, NIST CSF, CIS, etc.)
  - Promote security as a business enabler
- Risk management
  - Identify, assess, and mitigate cyber risks
  - Use standard methodologies (ISO 27005, NIST RMF)
  - Define *risk appetite(1) and tolerance* with the board

(1) propensione al rischio

CISO’s work (2)

- Compliance
  - Understand compelling laws and regulation like GDPR, NIS2, etc.
  - Ensure compliance (or delegate to specific professional)
  - Manage internal and external audits
  - Demonstrate accountability: keep track of taken actions
  - Demonstrate due diligence: keep track of decision process
- Security Policies and Processes
  - Establish and maintain key security policies
  - Ensure integration into company processes
  - Review and update policies periodically

CISO’s work (3)

- Organization
  - Define responsibilities (CISO, DPO, SOC, IT, …)
  - Promote shared responsibility
  - Foster security culture through training and awareness
- Incident Response and Business Continuity
  - Incident Response Plans (possibly according to a standard)
  - Plan and Coordinate with *disaster recovery* and *business continuity*
  - Manage crisis communication internally and externally

CISO’s work (3)

- Monitoring and Metrics
  - Define and check Key Performance Indicators (KPI)
    - *KPI: measure performance*
    - E.g. % of critical assets covered by active security controls,
    - % of high-risk vulnerabilities remediated within SLA
    - average time to implement mandatory compliance controls (GDPR, NIS2)
    - % of business-critical services tested for resilience against cyberattacks.
  - Define and check Key Risk Indicators (KRI)
    - *KRI: Level of risk exposure*
    - E.g. Mean Time To Detection (MTTD), Mean Time To Response (MTTR), patching rate, etc.
  - Ensure continuous monitoring
  - Provide dashboards or reports for management

CISO’s work (4)

- Supply Chain & Third-Party Risk
  - Evaluate suppliers and vendors
  - Include security clauses in contracts
  - Mitigate risks of supply chain attacks
    - i.e. malware coming with a software update or from management software
- Innovation and Emerging Technologies
  - Governance in cloud, multi-cloud, and DevSecOps
  - Secure IoT and OT (Industry 4.0)
  - Address AI governance and risks

CISO’s work depends on the kind of company

Two big types of companies

- Companies that **use** cybersecurity services
  - Their core business is not cybersecurity.
  - Often lack in-house cybersecurity expertise.
  - Purchase various cybersecurity services from external providers.
- Companies that **provide** cybersecurity services
  - Their core business is cybersecurity.
  - Possess strong technical expertise in the field.
  - Sell a wide range of cybersecurity services to other organizations.

Cybersecurity-User Companies

- 🎯 Goal: protect the core business.

CISO’s work

- Translate **cyber risks into business risks**
- Manage compliance (GDPR, NIS2, etc.)
- Oversee and **select external providers**

Typical Profile

- Manager with strong governance and risk management skills
- Often an external or part-time CISO (a *virtual* CISO)

Cybersecurity-Provider Companies

- 🎯 Goal: deliver security as a product/service.

CISO’s work

- Ensure security of services/products
- Support sales and client relations
- Lead R&D on emerging threats

Typical Profile:

- Highly technical and authoritative figure
- Works closely with CTO and research teams

DPO’s work

- Deep knowledge of GDPR and other privacy-related laws
- Interact with government authorities
  - E.g. Italian “garante per la privacy”
- Guide other roles regarding organization obligations
  - Verify compliance (auditing)
- Evaluate privacy aspects in new or existing projects
  - Promote data protection by design & default
- Keep updated processing activity records (1)
- Supervise DPIA execution (Art. 35 GDPR), if needed
  - Data Protection Impact Assessment: Identify and mitigate high-risk processing
- Data Breach Management
  - Collaborate with CISO/CIO in incident response
  - Document all incidents and actions taken, notify to authorities

(1) Registro dei trattamenti dei dati personali

What is a Cybersecurity Framework?

Definition

- A cybersecurity framework is a structured set of…
  - guidelines,
  - best practices,
  - standards, and
  - processes..
- …that helps organizations to…
  - identify and assess cybersecurity risks
  - protect critical assets and data
  - detect, respond to, and recover from cyber incidents
  - align cybersecurity activities with business objectives

- Frameworks help companies to avoid re-inventing well established practices reducing costs

Key Characteristics

- Structured: Organized into categories, functions, or domains
- Risk-Based: Focused on significant threats first
- Flexible / Scalable: Applies to organizations of different sizes
- Auditable / Measurable: Provides KPIs/KRIs
- Integrative: Can map to regulations and standards

Core Components

- Functions / Domains
  - e.g. from NIST CSF Identify, Protect, Detect, Respond, Recover
- Categories / Subcategories
  - e.g., Access Control, Vulnerability Management
- **Controls** / Practices
  - MFA, Firewalls, Patching Procedures
- Metrics / Indicators
  - KPIs and KRIs
- Maturity / Implementation Levels
  - Benchmarking and posture improvement

Benefits of Using a Cybersecurity Framework

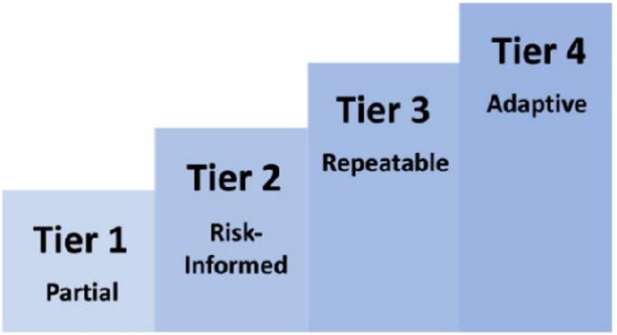
- Consistency: Standardizes practices
- Risk Management: Prioritizes critical risks
- Compliance Alignment: Helps satisfy regulations
- Communication: Common language for teams and board
- Continuous Improvement: Regular review and refinement

Examples of Cybersecurity Frameworks

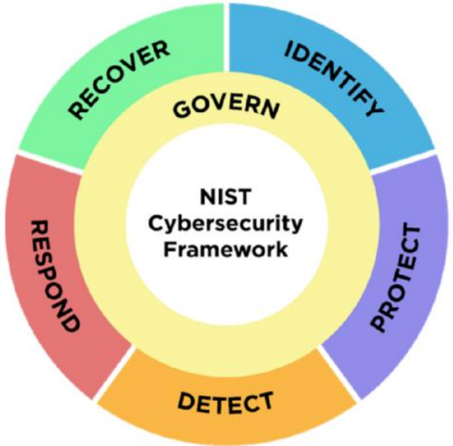
- NIST CSF: High-level functions, **widely used**
- ISO/IEC 27000 series: ISMS-focused, **certifiable**
- CIS Controls: Practical, prioritized **technical** controls
- COBIT: Governance-oriented, aligns IT and business

NIST CyberSecurity Framework (CSF)

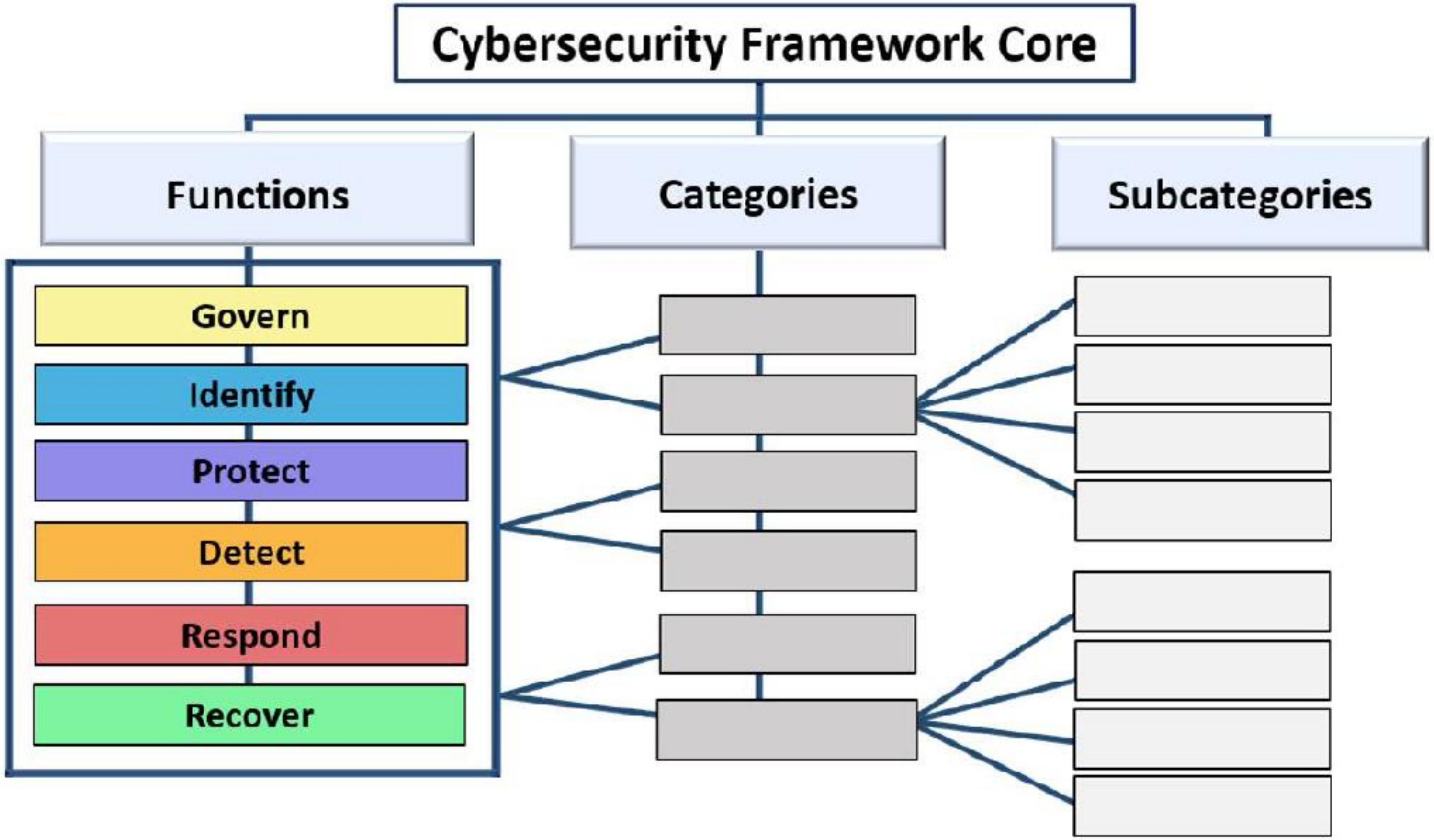
- By National Institute of Standards and Technology
- Publicly available
- Incremental adoption (tiers)



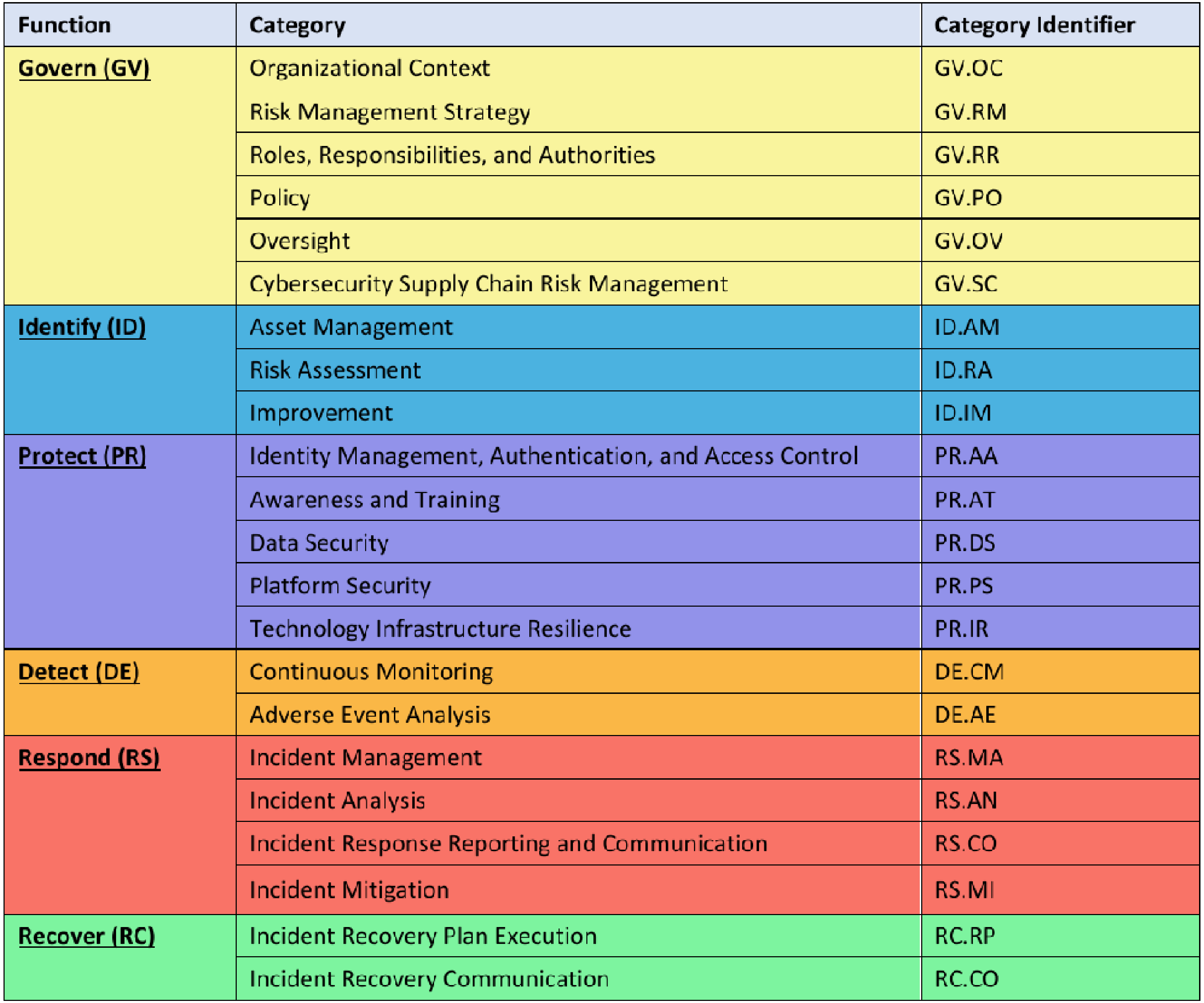
- Customizable to specific companies or situations (profiles)
- 6 core functions



NIST CSF


Cybersecurity Framework Core
Functions
Categories
Subcategories
Govern
Identify
Protect
Detect
Respond
Recover

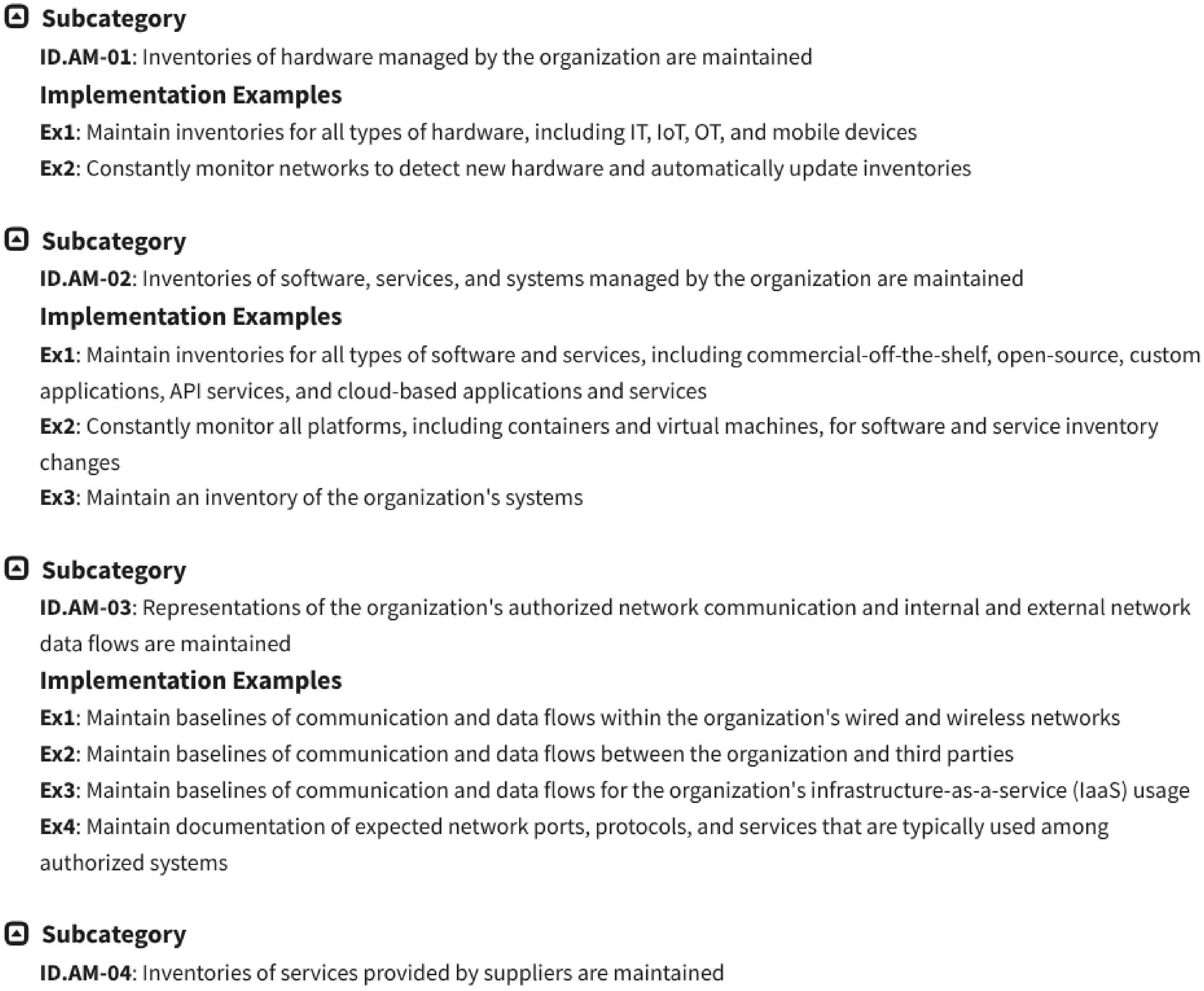
NIST CSF 2.0



Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Subcategories examples

Identify, Access Management



⏶ **Subcategory**

ID.AM-01: Inventories of hardware managed by the organization are maintained

Implementation Examples

Ex1: Maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices

Ex2: Constantly monitor networks to detect new hardware and automatically update inventories

⏶ **Subcategory**

ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained

Implementation Examples

Ex1: Maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services

Ex2: Constantly monitor all platforms, including containers and virtual machines, for software and service inventory changes

Ex3: Maintain an inventory of the organization's systems

⏶ **Subcategory**

ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained

Implementation Examples

Ex1: Maintain baselines of communication and data flows within the organization's wired and wireless networks

Ex2: Maintain baselines of communication and data flows between the organization and third parties

Ex3: Maintain baselines of communication and data flows for the organization's infrastructure-as-a-service (IaaS) usage

Ex4: Maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems

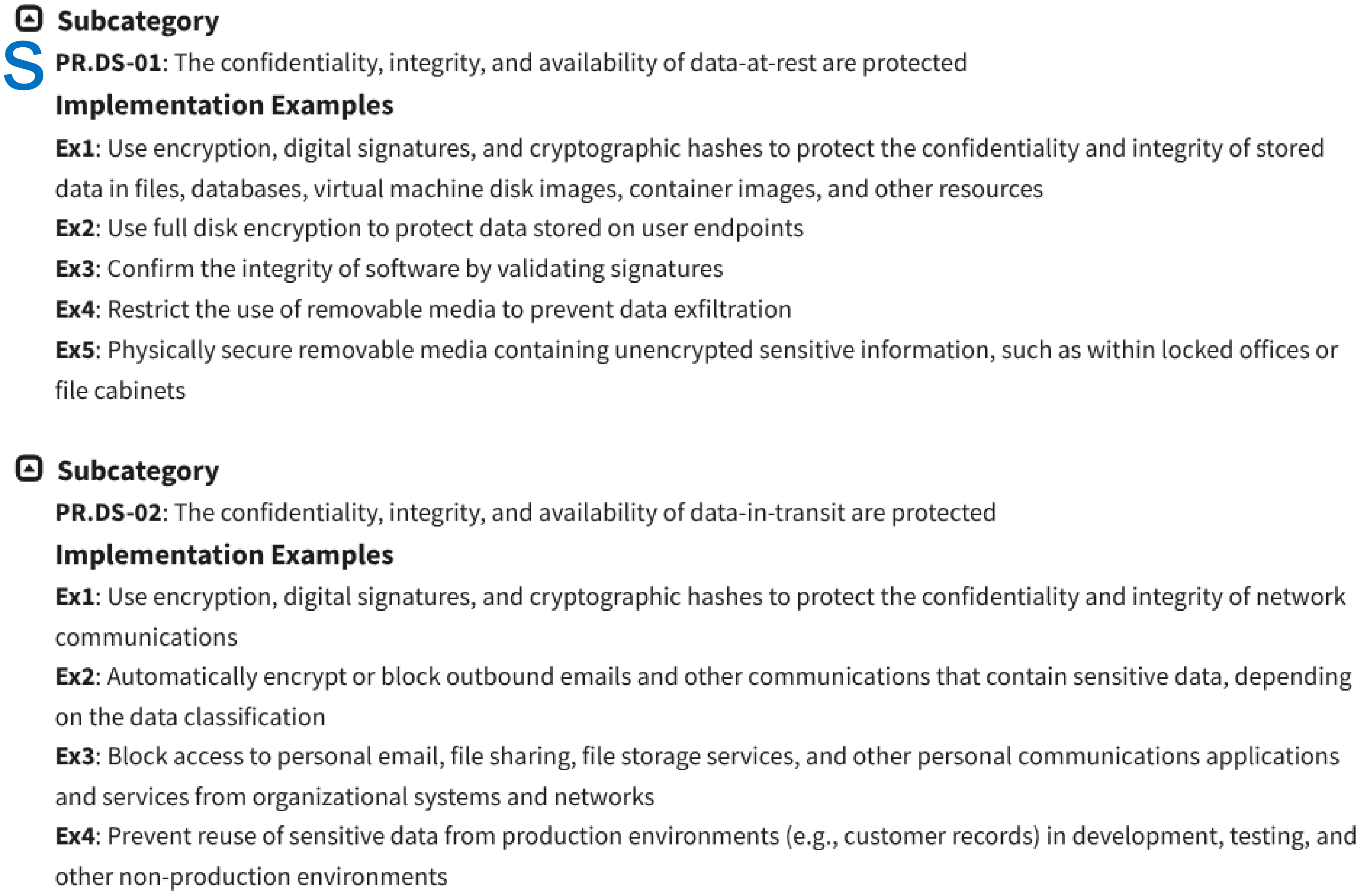
⏶ **Subcategory**

ID.AM-04: Inventories of services provided by suppliers are maintained

- https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

Subcategories examples

Protect, Data Security



Subcategory

PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected

Implementation Examples

Ex1: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources

Ex2: Use full disk encryption to protect data stored on user endpoints

Ex3: Confirm the integrity of software by validating signatures

Ex4: Restrict the use of removable media to prevent data exfiltration

Ex5: Physically secure removable media containing unencrypted sensitive information, such as within locked offices or file cabinets

Subcategory

PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected

Implementation Examples

Ex1: Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of network communications

Ex2: Automatically encrypt or block outbound emails and other communications that contain sensitive data, depending on the data classification

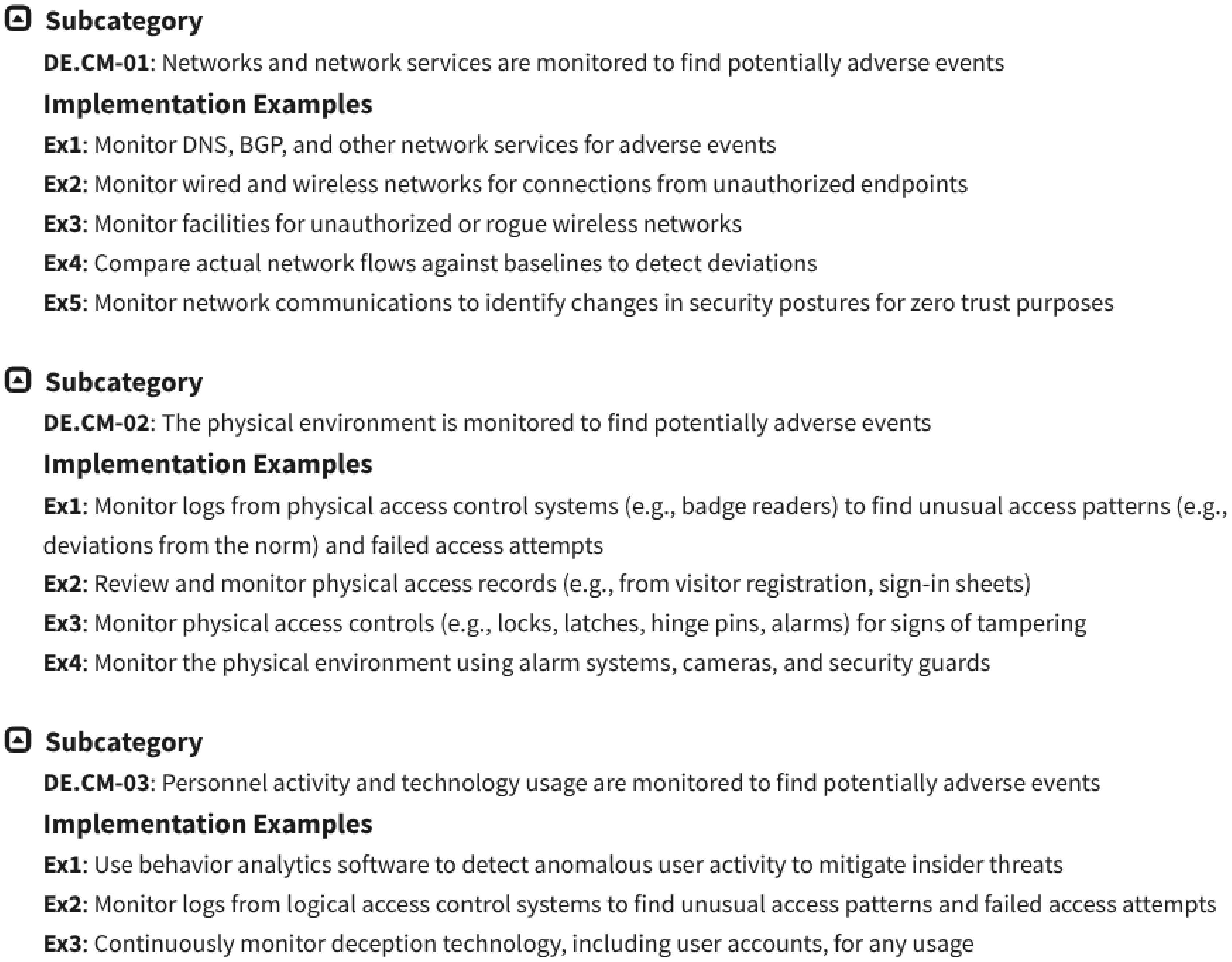
Ex3: Block access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems and networks

Ex4: Prevent reuse of sensitive data from production environments (e.g., customer records) in development, testing, and other non-production environments

- https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

Subcategories examples

Detect, Continuous Monitoring



Subcategory

DE.CM-01: Networks and network services are monitored to find potentially adverse events

Implementation Examples

Ex1: Monitor DNS, BGP, and other network services for adverse events

Ex2: Monitor wired and wireless networks for connections from unauthorized endpoints

Ex3: Monitor facilities for unauthorized or rogue wireless networks

Ex4: Compare actual network flows against baselines to detect deviations

Ex5: Monitor network communications to identify changes in security postures for zero trust purposes

Subcategory

DE.CM-02: The physical environment is monitored to find potentially adverse events

Implementation Examples

Ex1: Monitor logs from physical access control systems (e.g., badge readers) to find unusual access patterns (e.g., deviations from the norm) and failed access attempts

Ex2: Review and monitor physical access records (e.g., from visitor registration, sign-in sheets)

Ex3: Monitor physical access controls (e.g., locks, latches, hinge pins, alarms) for signs of tampering

Ex4: Monitor the physical environment using alarm systems, cameras, and security guards

Subcategory

DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events

Implementation Examples

Ex1: Use behavior analytics software to detect anomalous user activity to mitigate insider threats

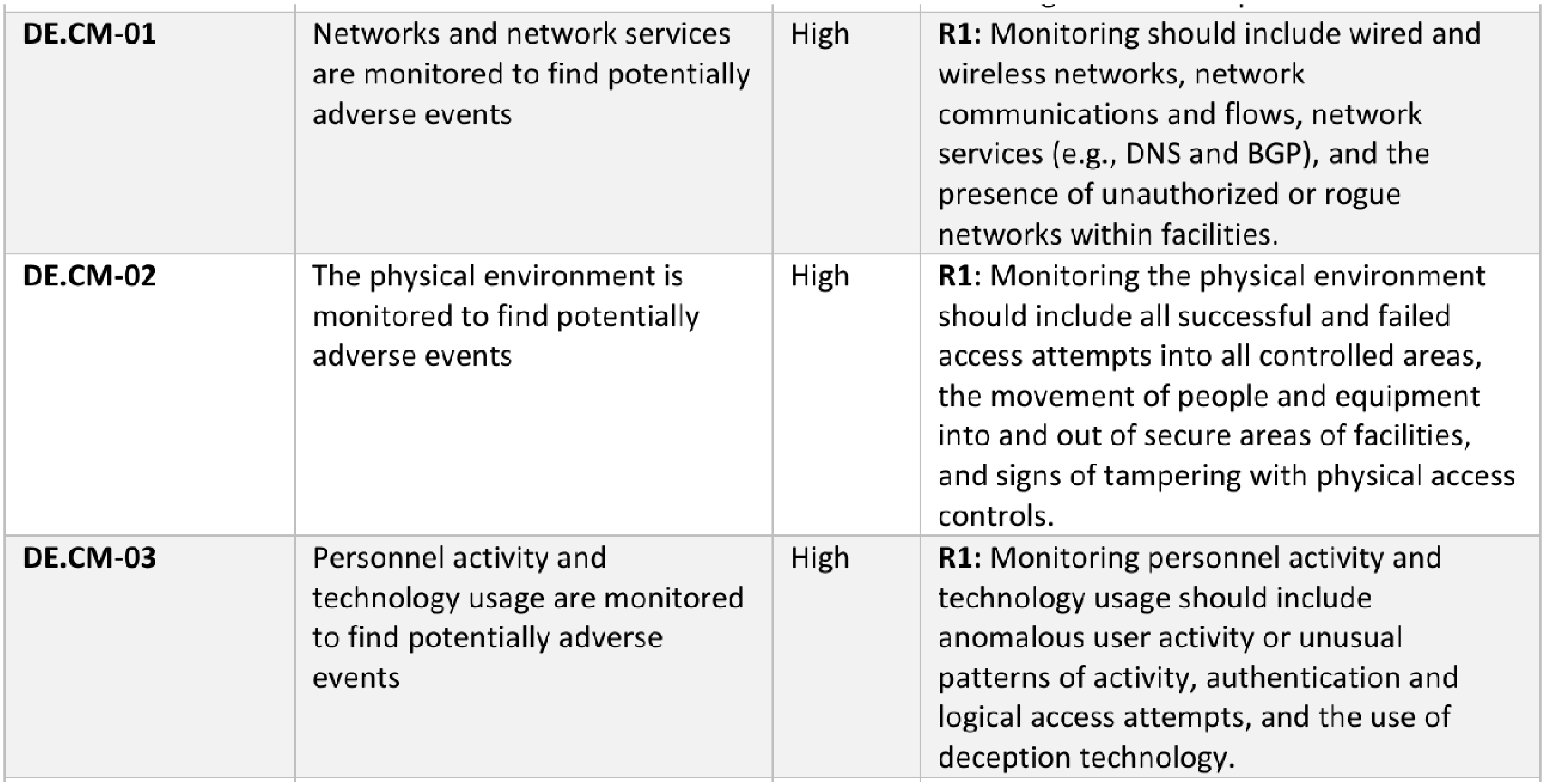
Ex2: Monitor logs from logical access control systems to find unusual access patterns and failed access attempts

Ex3: Continuously monitor deception technology, including user accounts, for any usage

- https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters

NIST profile example

(incident response)



DE.CM-01	Networks and network services are monitored to find potentially adverse events	High	**R1:** Monitoring should include wired and wireless networks, network communications and flows, network services (e.g., DNS and BGP), and the presence of unauthorized or rogue networks within facilities.
DE.CM-02	The physical environment is monitored to find potentially adverse events	High	**R1**: Monitoring the physical environment should include all successful and failed access attempts into all controlled areas, the movement of people and equipment into and out of secure areas of facilities, and signs of tampering with physical access controls.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	High	**R1:** Monitoring personnel activity and technology usage should include anomalous user activity or unusual patterns of activity, authentication and logical access attempts, and the use of deception technology.

NIST SP 800-53

- Security and Privacy Controls for Federal Information Systems and Organizations
- **Independent from NIST CSF!!!!**

- It contains technical controls, discussed
  - about 900
- Very technical and detailed
- Manadatory for US federal administration
- Publicly available

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Framework Nazionale per la Cybersecurity e la Data Protection

- Ispirato a NIST CSF + conformità alla normativa italiana

ISO27000 series

- **ISO 27000** – Vocabulary & overview
- **ISO 27001** – ISMS requirements (**certifiable**)
- **ISO 27002** – Controls guidance (best practices)
  - Similar to NIST CSF for scope and abstraction
- **Other ISO 2700x** – Specialized guidance for auditing, risk management, cloud, incident management, privacy, and sector-specific use
- Not publicly available

Building and Operating an ISMS

- **Define the Information Security Governance Structure**
  - Establish roles and responsibilities (CISO, process owners, top management)
  - Define the security policy and security objectives
  - Set up committees and escalation processes
- **Understand the Organization's Context**
  - Analyze **what the organization does**
  - Identify **legal and regulatory requirements**
  - Identify interested **parties** and their expectations
  - Determine which information **assets** need protection

Building and Operating an ISMS

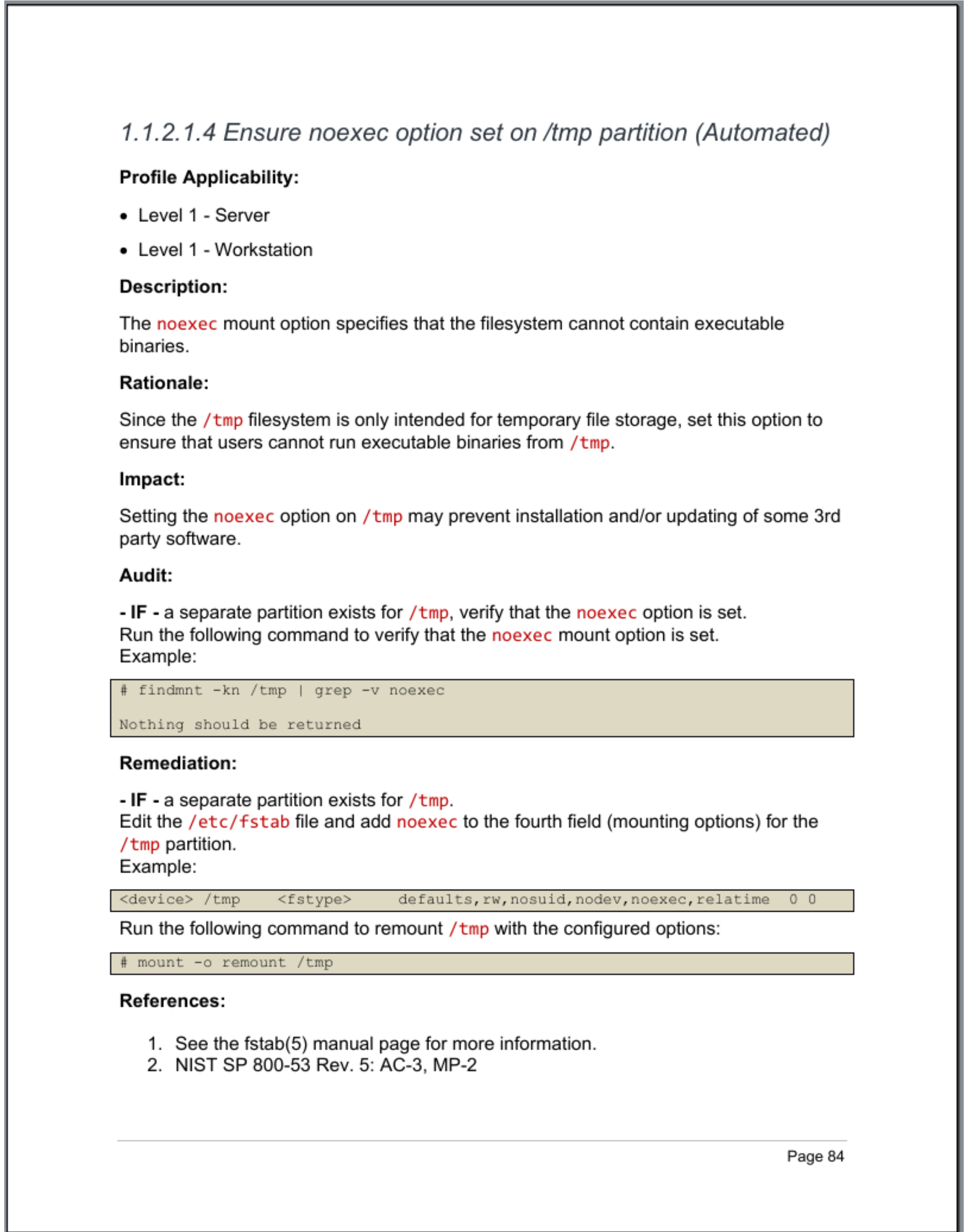
- **Define the Scope of the ISMS**
  - Clarify **boundaries** and applicability of the ISMS
  - Decide which processes, locations, people, and technologies are included
- **Apply Risk Management**
  - Identify assets, threats, and vulnerabilities
  - Assess risks (likelihood × impact)
  - Define risk treatment measures

Building and Operating an ISMS

- **Select and Implement Security Controls (Annex A / ISO 27002)**
- **Document the ISMS**
  - – Several mandatory documents
- **Activate Operational Security Processes**
  - – The ISMS must **operate continuously**, not only on paper.
- **Monitor, Measure, and Continually Improve**
  - – KPIs, KRIs, internal audits, management reviews
  - – Apply corrective actions (Plan-Do-Check-Act cycle)

CIS Benchmarks

- Center for Internet Security (CIS)
  - Non-profit organization
- Collect internet best practices
- Very technical and targeted to common OS and software
- **Can be (largely) Automated**
  - **Check**
  - **Remediation**
- Publicly available upon request



1.1.2.1.4 Ensure noexec option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/tmp`.

Impact:

Setting the `noexec` option on `/tmp` may prevent installation and/or updating of some 3rd party software.

Audit:

- IF - a separate partition exists for `/tmp`, verify that the `noexec` option is set.
Run the following command to verify that the `noexec` mount option is set.
Example:

```
# findmnt -kn /tmp | grep -v noexec

Nothing should be returned
```

Remediation:

- IF - a separate partition exists for `/tmp`.
Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition.
Example:

```
<device> /tmp    <fstype>     defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

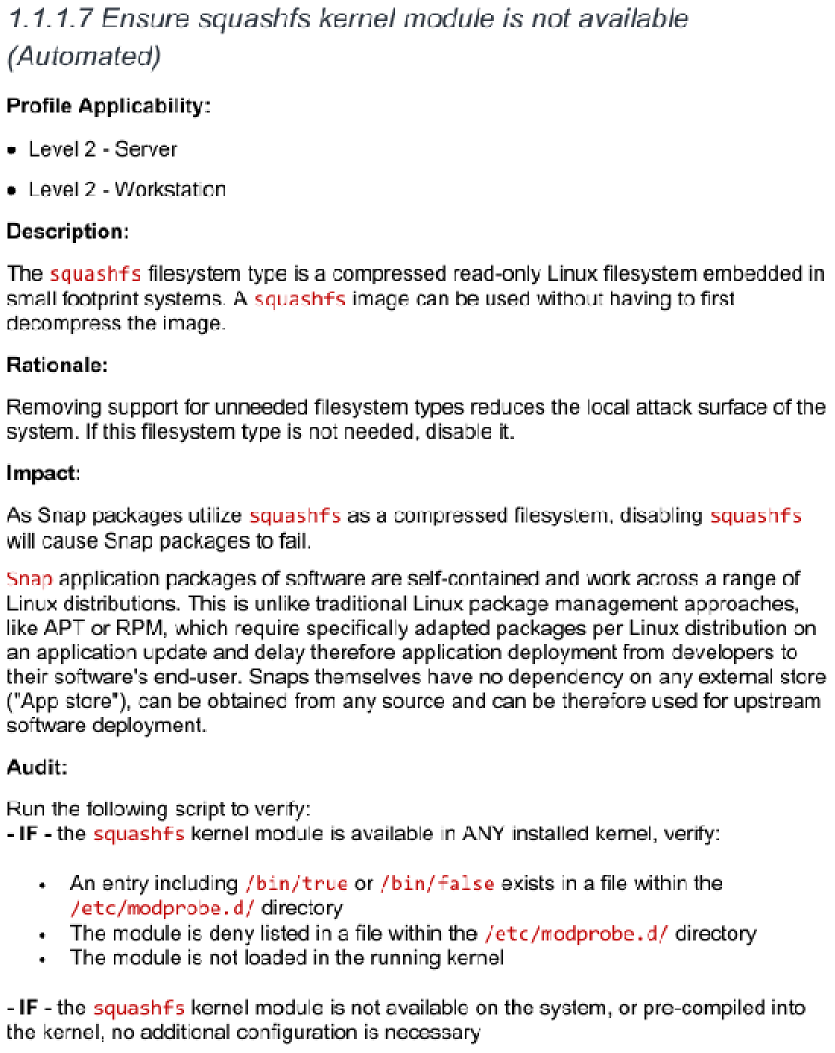
```
# mount -o remount /tmp
```

References:

1. See the fstab(5) manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

Page 84

CIS Benchmarks



1.1.1.7 Ensure squashfs kernel module is not available (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `squashfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `squashfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Impact:

As Snap packages utilize `squashfs` as a compressed filesystem, disabling `squashfs` will cause Snap packages to fail.

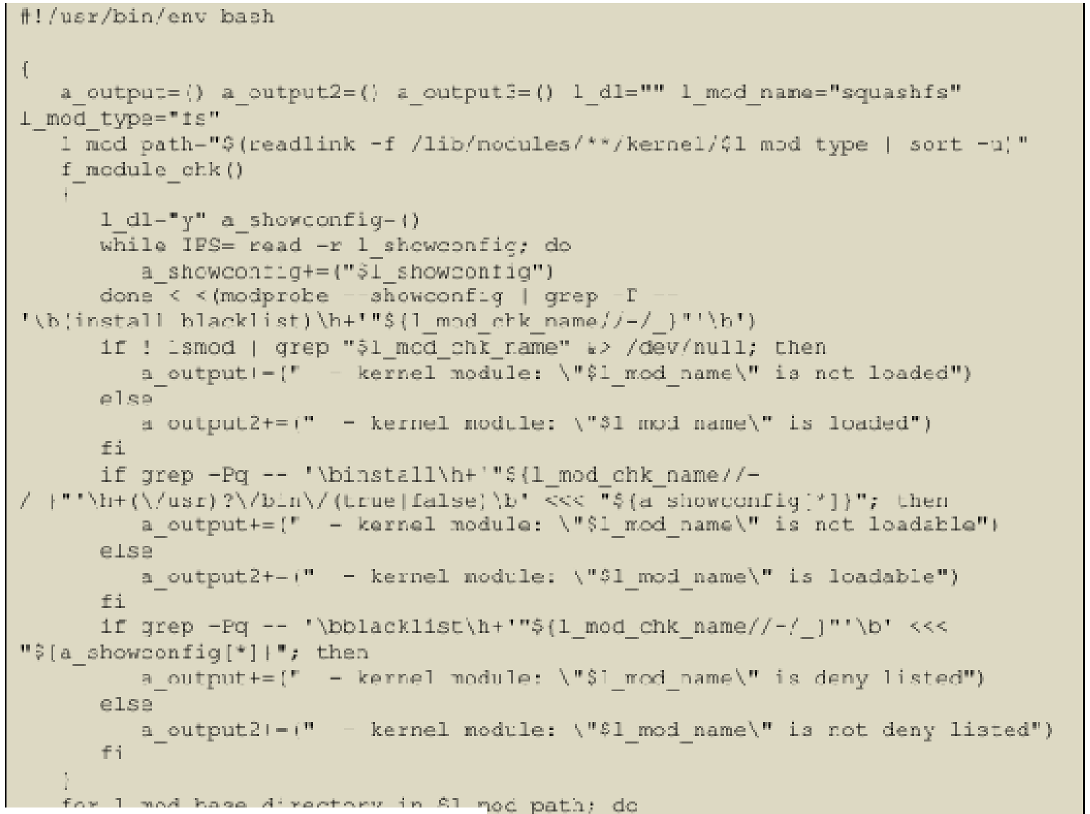
`Snap` application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment.

Audit:

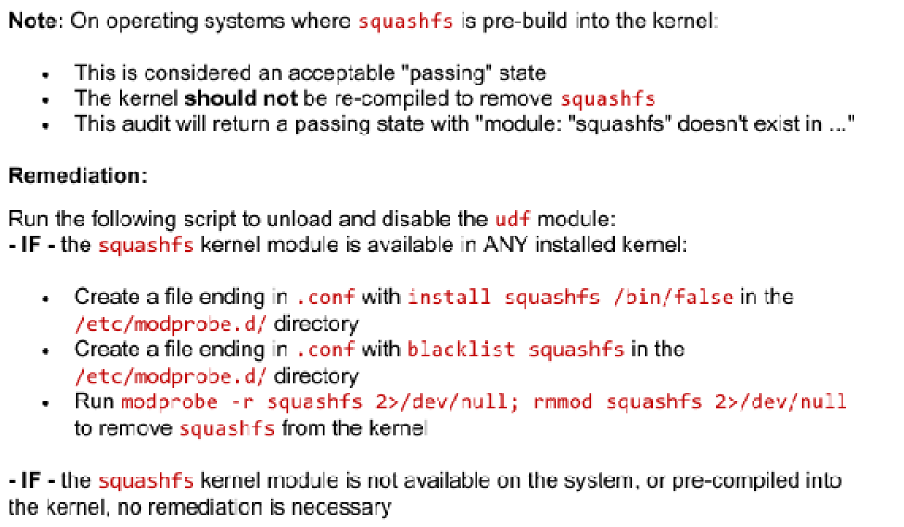
Run the following script to verify:
- IF - the `squashfs` kernel module is available in ANY installed kernel, verify:

- An entry including `/bin/true` or `/bin/false` exists in a file within the `/etc/modprobe.d/` directory
- The module is deny listed in a file within the `/etc/modprobe.d/` directory
- The module is not loaded in the running kernel

- IF - the `squashfs` kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary



```
#!/usr/bin/env bash

{
   a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="squashfs"
l_mod_type="fs"
   l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
   f_module_chk()
   {
      l_dl="y" a_showconfig=()
      while IFS= read -r l_showconfig; do
         a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'"${l_mod_chk_name//-/_}"'\b')
      if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
         a_output+=("  - kernel module: \"$l_mod_name\" is not loaded")
      else
         a_output2+=("  - kernel module: \"$l_mod_name\" is loaded")
      fi
      if grep -Pq -- '\binstall\h+'"${l_mod_chk_name//-
/_}"'\h+(\/usr)?\/bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
         a_output+=("  - kernel module: \"$l_mod_name\" is not loadable")
      else
         a_output2+=("  - kernel module: \"$l_mod_name\" is loadable")
      fi
      if grep -Pq -- '\bblacklist\h+'"${l_mod_chk_name//-/_}"'\b' <<<
"${a_showconfig[*]}"; then
         a_output+=("  - kernel module: \"$l_mod_name\" is deny listed")
      else
         a_output2+=("  - kernel module: \"$l_mod_name\" is not deny listed")
      fi
   }
   for l_mod_base_directory in $l_mod_path; do
                                       y/${l_mod_name/-/\/}" ] && [ -n "$(ls -A
                                       e/-/\/}")" ]; then
                                        base_directory\"")
                                       e"
                                       y ]] && l_mod_chk_name="${l_mod_name::-2}"
                                       odule_chk

                                       le: \"$l_mod_name\" doesn't exist in



                                        printf '%s\n' "" "  -- INFO --" "  - module:
                                       tput3[@]}"
                                         then
                                       ult:" "  ** PASS **" "${a_output[@]}"

                                       ult:" "  ** FAIL **" "  - Reason(s) for

                                       & printf '%s\n' "- Correctly set:"
```



Note: On operating systems where `squashfs` is pre-build into the kernel:

- This is considered an acceptable "passing" state
- The kernel **should not** be re-compiled to remove `squashfs`
- This audit will return a passing state with "module: "squashfs" doesn't exist in ..."

Remediation:

Run the following script to unload and disable the `udf` module:
- IF - the `squashfs` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install squashfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist squashfs` in the `/etc/modprobe.d/` directory
- Run `modprobe -r squashfs 2>/dev/null; rmmod squashfs 2>/dev/null` to remove `squashfs` from the kernel

- IF - the `squashfs` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

Regulatory Compliance

Regulatory Compliance

- One of the main objective of governance is compliance with regulation, standards or practices

Main cybersecurity regulations relevant for Italy

- General Data Protection Regulation, **GDPR** (EU) 2016/679
- Network and Information Security Directive 2 **NIS2** (EU Directive 2022/2555)
- Perimetro di Sicurezza Nazionale Cibernetica, **PSNC** Decree-Law 105/2019
- Digital Operational Resilience Act, **DORA** (UE 2022/2554)

Common Regulatory Contents

- Scope of Application
  - Which companies are affected?
  - Which business processes are included?
- ICT Risk Management
  - Risk identification and mitigation
- Governance and Accountability
  - Who is responsible?
- What governing body oversees compliance?
  - Incident Notification and Management
  - Reporting to supervisory or governmental authorities
- Operational Resilience Testing
  - Regular assessments of ICT systems and procedures
- ICT Supplier Evaluation
  - Compliance assessment of third-party ICT providers
- Penalties for Non-Compliance
  - Sanctions and consequences for failure to comply

comparazione tra alcune normative rilevanti in italia

Aspetto	GDPR (UE 2016/679)	NIS2 (Direttiva UE 2022/2555)	PSNC (D.L. 105/2019)	DORA (UE 2022/2554)
Obiettivo	Protezione dati personali (privacy)	Sicurezza reti e sistemi critici	Sicurezza nazionale	Resilienza digitale finanziaria
Settore applicazione	Tutti i settori	Settori critici generali	Entità di interesse nazionale	Settore finanziario
Gestione del rischio ICT	Obbligatoria di fatto	Obbligatoria	Obbligatoria	Obbligatoria
Responsabilità della governance	Titolare del trattamento	Dirigenza	Dirigenza	Dirigenza
Notifica incidenti	Violazioni dei dati personali	Per i più rilevanti	Incidenti rilevanti	Per i più rilevanti
Test di resilienza	Non specificato	Raccomandati	Non specificato	Obbligatori
Valutazione/verifica fornitori ICT	Non specificato	Obbligatoria	Obbligatoria	Obbligatoria
Sanzioni per inadempimento	Fino a €20M o 4% fatturato	Sanzioni fino a 10M € o 2% fatturato	Sanzioni fino a 1.8M€ (x3), reclusione, interdizione	varia per Stato

Other GDPR Obligations

- Accountability
  - Data controllers must demonstrate compliance with the GDPR and document every measure taken.
- Record of Processing Activities (Art. 30)
  - Maintain an up-to-date record of processing activities: purposes, data categories, data subjects, recipients, retention periods, and security measures.
- Privacy by Design and by Default (Art. 25)
  - Integrate data protection from the design stage of systems and processes.
  - Collect and process only the minimum necessary data.
- Transparency and Consent (Arts. 12–14, 7)
  - Provide clear, accessible privacy notices to data subjects and obtain explicit, documented consent
- Data Subject Rights (Arts. 15–22)
  - Access, Rectification, Erasure (“right to be forgotten”), Restriction, Data portability, Objection, No fully automated decisions without consent
- Data Protection Impact Assessment – DPIA (Art. 35)
  - Required for processing that poses high risk (e.g., video surveillance, profiling, biometric data). Includes risk analysis, mitigation measures, and, if needed, prior consultation of the Data Protection Autority (e.g. “Garante della Privacy”)
- Data Protection Officer (DPO) Appointment (Art. 37)
  - Mandatory for Public authorities/organizations; Entities processing large-scale sensitive data or systematically monitoring people.

NIS2 Scope (focus on EU)

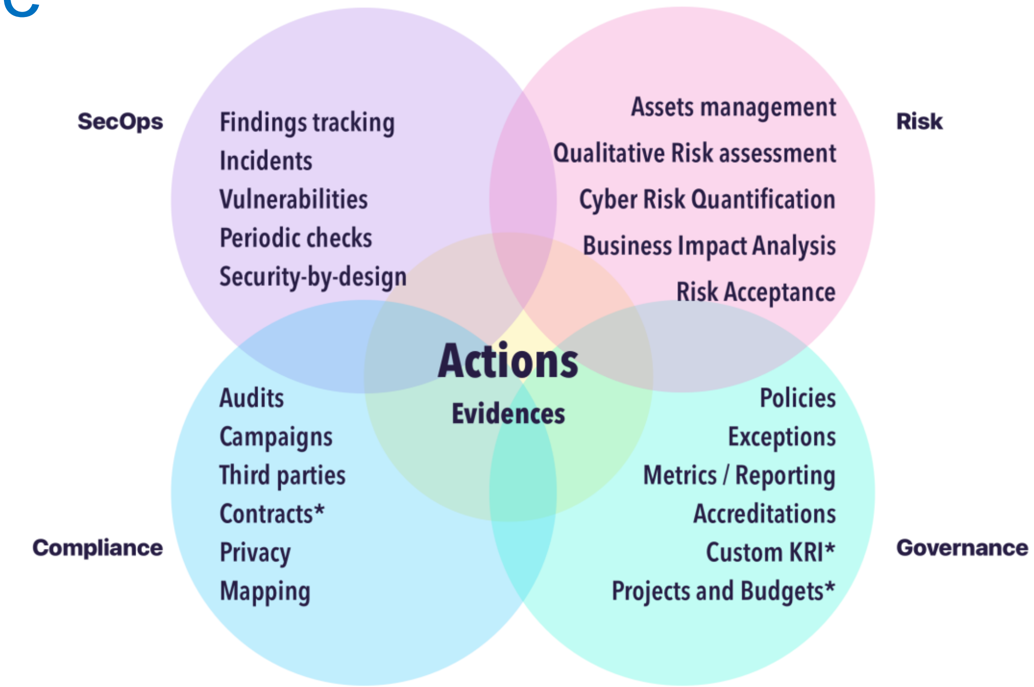
- Essential Entities:
  - Critical sectors for society and the economy, including: Energy (electricity, gas, oil), Transport (air, rail, maritime, road), Banks and critical financial infrastructures, Capital markets and payment infrastructures, Health (hospitals, laboratories, pharmacies), Drinking water, Digital infrastructure (ISPs, DNS, critical cloud services), Public administration
- Important Entities
  - Sectors of economic relevance but not necessarily critical for national security: Food and agriculture, Chemical industry, Waste management, Digital service providers not classified as critical
- Inclusion criteria: large or medium-sized companies included in important or essential entities operating in EU or serving EU.
  - Small enterprises are usually excluded

PSNC

- Simile in scopo a NIS2 ma con l’obiettivo di proteggere la sicurezza cibernetica nazionale italiana
- Più stringente di NIS2
- Se una organizzazione ricade in PSNC non deve essere conforme anche a NIS2
  - Nella norma di recepimento della direttiva NIS2: D.Lgs. 138/2024, art. 33

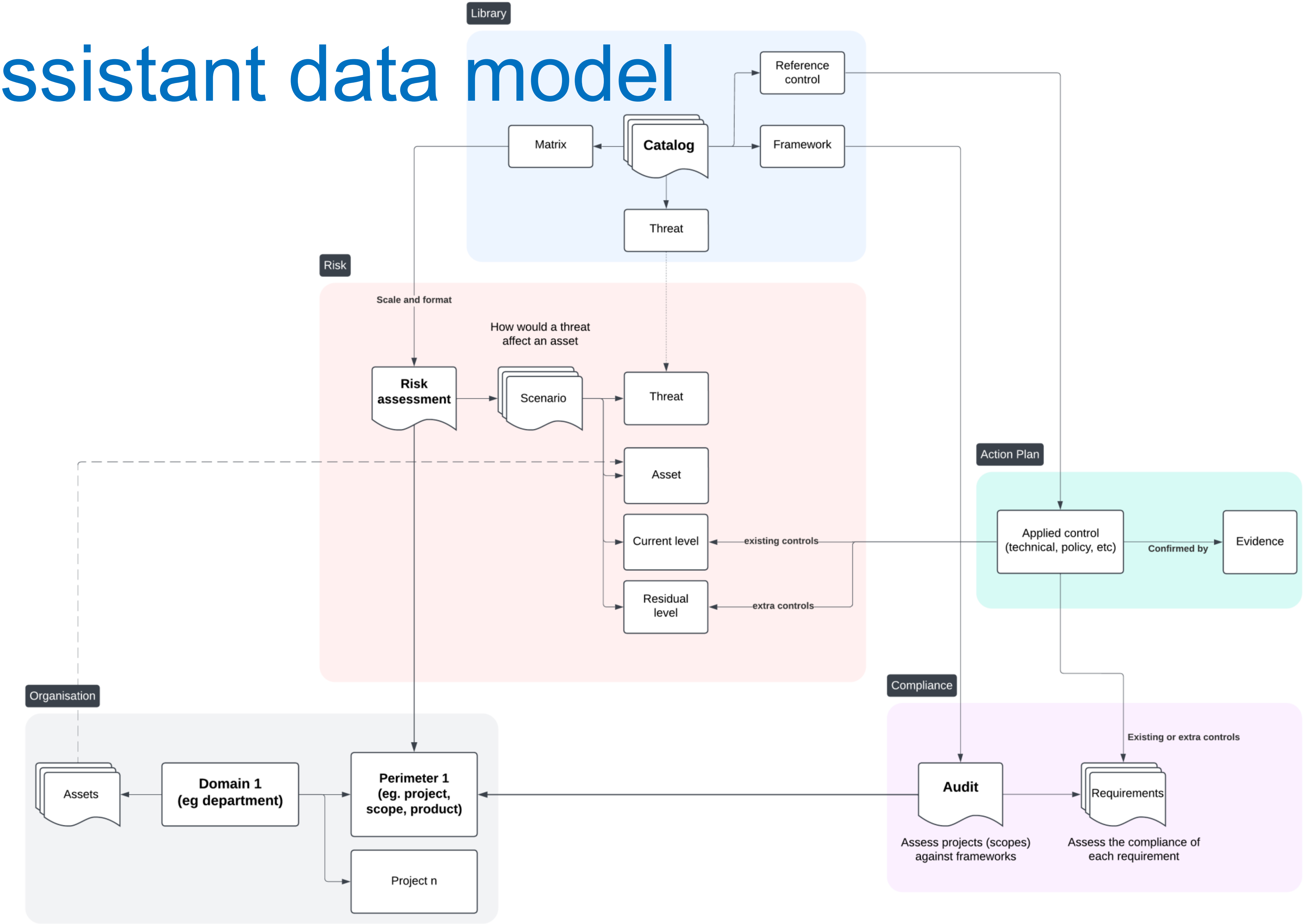
Free “CISO support tools”

- CISO Assistant
  - https://github.com/intuitem/ciso-assistant-community
  - open source



- OpenGRC
  - https://github.com/LeeMangold/OpenGRC/
  - open source with some restrictions

Ciso Assistant data model


Library
Reference control
Matrix
Catalog
Framework
Threat
Risk
Scale and format
How would a threat affect an asset
Risk assessment
Scenario
Threat
Asset
Current level
existing controls
Residual level
extra controls
Action Plan
Applied control (technical, policy, etc)
Confirmed by
Evidence
Compliance
Existing or extra controls
Organisation
Assets
Domain 1 (eg department)
Perimeter 1 (eg. project, scope, product)
Project n
Audit
Requirements
Assess projects (scopes) against frameworks
Assess the compliance of each requirement