Security Governance
Master of Science in Cyber Security

AY 2025-26

CYBERSECURITY FRAMEWORKS AND BEST PRACTICES

What is a Cybersecurity Framework?

A structured set of guidelines, best practices, and standards for managing cybersecurity risks

Purpose: Provides a roadmap to assess, improve, and communicate security posture.

Key Traits

- Standardized approach
- Risk-based and adaptable
- Continuous improvement

Examples

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001 & 27002
- CIS Controls
- COBIT

A bit of History

In USA in 2014, President Obama defines the Cybersecurity Enhancement Act of 2014 (CEA)

- It updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators

Through CEA, NIST must identify
*"a prioritized, flexible, repeatable, performance-based, and cost-effective **approach**, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage **cyber risks**"*.

CEA formalizes NIST's previous work[1] and provided guidance for future Framework evolution.

1- Framework Version 1.0 under Executive Order (EO) 13636, "*Improving Critical Infrastructure Cybersecurity*" (February 2013)

NIST CSF

The Framework

- focuses on using **business drivers** to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.
- consists of three parts:
  1. Core
  2. Implementation Tiers
  3. Profiles

Applicability of NIST CSF

- NIST CSF was developed to improve cybersecurity risk management in critical infrastructures, but it can be used by organizations in any sector or community
- It provides a common organizing structure assembling standards, guidelines, and practices that are working effectively today
- It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on
  - information technology (IT),
  - industrial control systems (ICS)
  - cyber-physical systems (CPS)
  - connected devices more generally, including the Internet of Things (IoT)

NIST CSF Features

NIST CSF is technology neutral

- It remains effective and supports technical innovation

It references a variety of existing standards, guidelines, and practices that evolve with technology.

It provides a **common taxonomy** and **mechanism** for organizations to:

1.
2.
3.
4.
5.

NIST CSF supports cyber security assessment, planning and monitoring activities

Risk Management and CSF

RECALL: Risk management is the ongoing process of identifying, assessing, and responding to risk.

To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts.

With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.

NIST CSF Core

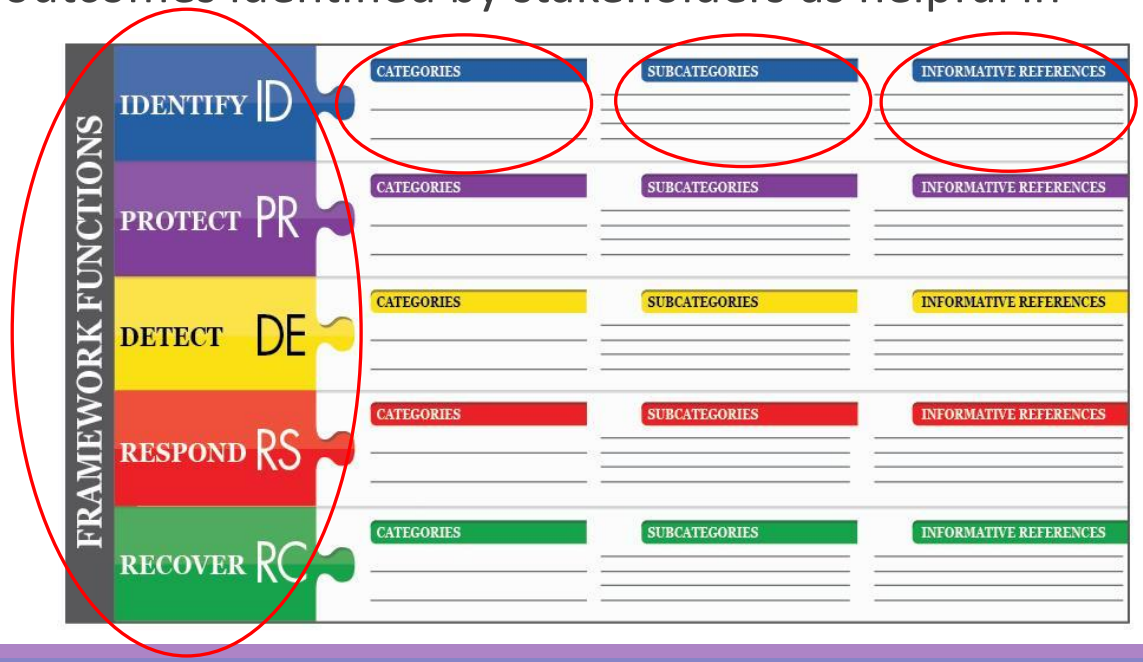
It provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

The Core is not a checklist of actions to perform.

It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk.

The Core comprises four elements:

1. Functions
2. Categories
3. Subcategories
4. Informative References



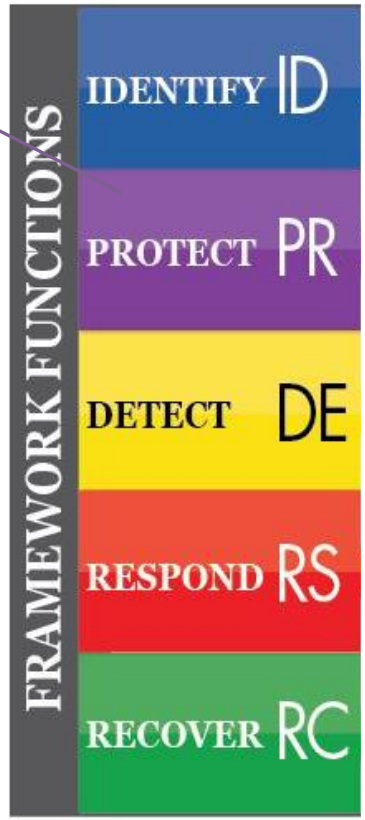
NIST CSF Core - Functions

Functions organize basic cybersecurity activities at their highest level.

Develop and implement appropriate safeguards to ensure delivery of critical services.

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident



Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST CSF Core – Other Elements

Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to **programmatic needs** and **particular activities**.

- Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”

Subcategories further divide a Category into **specific outcomes** of technical and/or management activities.

- They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category.
- Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a **method to achieve the outcomes** associated with each Subcategory.

Example - Identify

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9

Example - Protect

	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2

Example - Detect

	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Example - Respond

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8

Example - Recover

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") provide context on **how an organization views cybersecurity risk** and the **processes in place to manage that risk**

Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.

NOTE While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels.

- Tiers are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources.
- Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.

Framework Implementation Tiers

	Risk Management Process	Integrated Risk Management Program	External Participation
TIER 1 Partial	- Lack of formalization - ad hoc and sometimes reactive management - Prioritization of activities may not be directly based on by organizational risk objectives, the threat environment, or business/mission requirements	- limited awareness of cybersecurity risk at the organizational level - irregular, case-by-case basis due to varied experience or information gained from outside sources - The organization may not have in place information sharing processes	No collaboration

Framework Implementation Tiers

	Risk Management Process	Integrated Risk Management Program	External Participation
TIER 2 Risk Informed	- Management approval but possible absence of clear policies - Prioritization of activities may not be directly based on by organizational risk objectives	- awareness of cybersecurity risk at the organizational level but not an organization-wide approach to managing cybersecurity - information sharing within the organization on an informal basis. - not all levels of the organization are involved - Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.	Low Collaboration

Framework Implementation Tiers

	Risk Management Process	Integrated Risk Management Program	External Participation
TIER 3 Repeatable	- formal approval and definition of policy. - regularly updated	- There is an organization-wide approach to manage cybersecurity risk.	High Collaboration
TIER 4 Adaptive	- Standards and best Practices are applied - Continuous improvement process	- There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events	Full Collaboration

Framework Profile

The Framework Profile (“Profile”) is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization.

They can be used to describe the current state or the desired target state of specific cybersecurity activities.

- The Current Profile indicates the cybersecurity outcomes that are currently being achieved.
- The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals.
- Support gap analysis

This Framework does not prescribe Profile templates, allowing for flexibility in implementation

How to Use the Framework

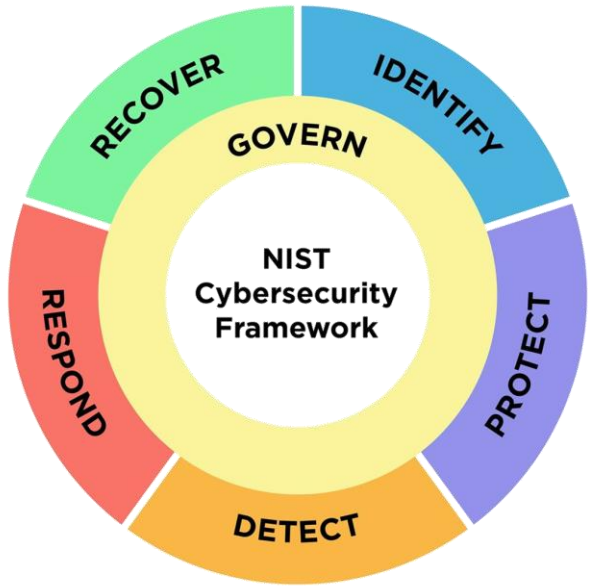
1. Basic Review of Cybersecurity Practices
2. Establishing or Improving a Cybersecurity Program
3. Communicating Cybersecurity Requirements with Stakeholders
4. Buying Decisions
5. Identifying Opportunities for New or Revised Informative References
6. Methodology to Protect Privacy and Civil Liberties
7. Self-Assessing Cybersecurity Risk with the Framework

CSF has been updated in 2023

- from 1 to 2
- why to update?
  - need for better governance in cybersecurity
  - adaptation to evolving threats and technological changes (e.g., supply chain risks, digital transformation)
  - improving alignment with international standards
  - focus on usability for organizations of various sizes and sectors

New ‘Govern’ Function in NIST CSF 2.0

- introduction of the sixth function: **Govern**
- key elements:
  - cybersecurity **governance**: roles, responsibilities, and structure
  - **policy development**: establishing and managing cybersecurity policies
  - **risk management strategy**: aligning cybersecurity risks with overall organizational risks
  - **resource allocation**: how to manage cybersecurity resources effectively
  - **compliance**: ensuring adherence to laws and regulations



Refinements to Existing Functions

- **identify**: expanded focus on risk management and critical assets
- **protect**: more specific guidelines on protecting critical infrastructure and data
- **detect**: refined detection technologies and threat intelligence
- **respond**: more detailed planning and communication strategies during incidents
- **recover**: greater emphasis on resilience and learning from past incidents

1.1

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

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

Enhanced Focus on Supply Chain Security

- greater emphasis on managing third-party risks
- new guidelines on vendor risk management and evaluating security in the supply chain

Global Alignment and Flexibility

- improved alignment with international cybersecurity standards (e.g., ISO, GDPR)
- flexibility for different types of organizations (small businesses, large enterprises, etc.)

Benefits of NIST CSF 2.0

- strengthened governance and oversight
- enhanced adaptability to evolving cyber threats
- better tools for compliance with regulations
- scalability for organizations of different sizes

Conclusion

- recap of the main updates in NIST CSF 2.0
- importance of implementing the **Govern** function
- encourage proactive adoption of NIST CSF 2.0 for improved cybersecurity resilience

National Cybersecurity Framework

Initial Objectives

Bring cyber risk awareness to the highest levels of the business

- No longer just a matter for technical staff
- Make organizations include cyber risk in risk management as part of an economic risk

Considering the Italian economic landscape

- 69% of the GDP is due to SME
- Very few large national enterprises: ~ 0.1%

Initial Objectives

Create something which is recognized at international level

- Improve information sharing capacity
- Increase the duty of care at the national level

Do not reinvent the wheel

- It makes no sense to create a new framework from scratch
- Use a recognized framework as a starting point:
  - NIST Framework for Improving Critical Infrastructure Cybersecurity

What the National Framework is and what is not

The National Framework is not a Standard

- It is not certifiable!

It is a tool for self-assessment

Allows organizations to assess their current cybersecurity posture («*current profile*») and define the desired one («*target profile*»)

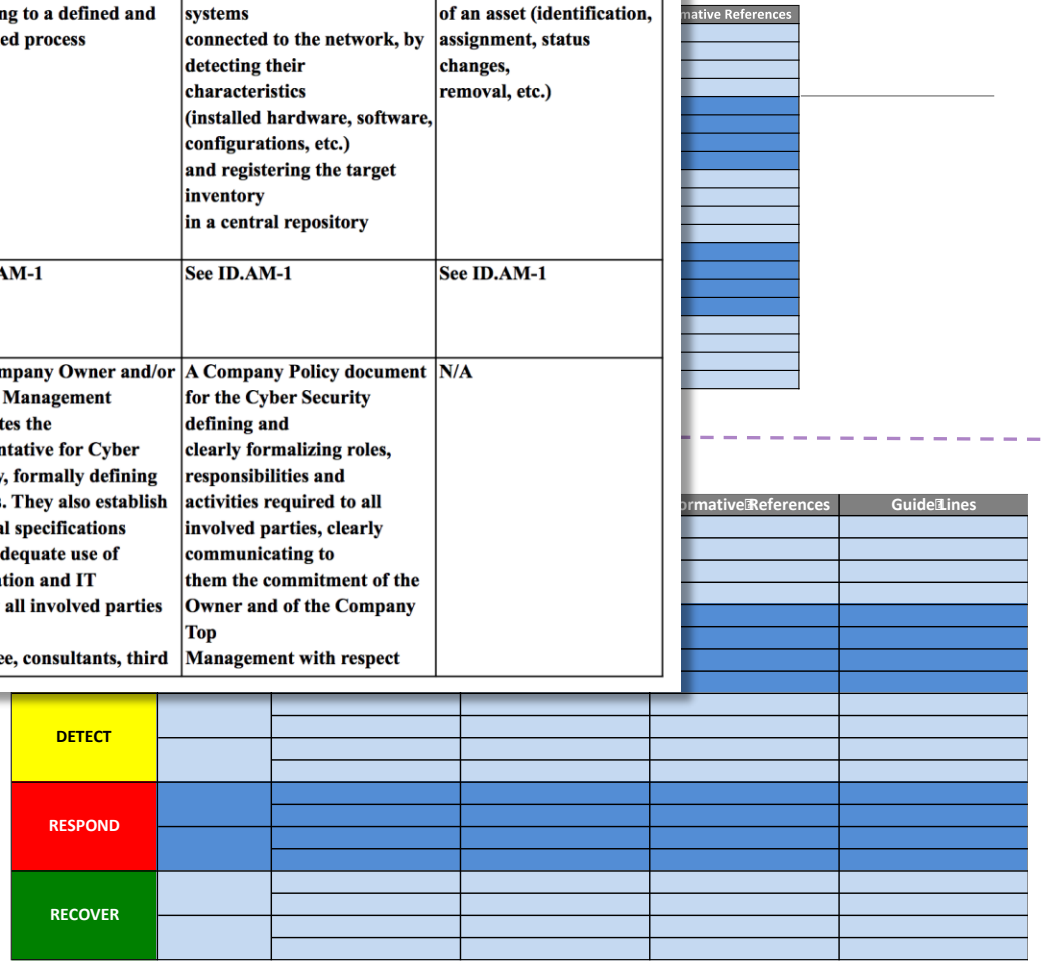
Support in the gap analysis and the definition of a roadmap to close the gap between the current and the target profile

From NIST CS Framework to Italian Na

Fram
Profil
Imple

- **Pr**
- **M**
  - Defined for each “contextualization”

Function	Subcategory	Reference to the Guide	Level 1	Level 2	Level 3
IDENTIFY (ID)	ID.AM-1: Physical devices and systems within the organization are inventoried	Table 6.1: Assets identification (IA)	Assets inventory, classification and update (intended as information, applications, available systems and equipment) are performed mainly manually according to a defined and controlled process	Assets inventory, classification and update are performed in part in automatic mode that allows at least to automate the "discovery" phase of systems connected to the network, by detecting their characteristics (installed hardware, software, configurations, etc.) and registering the target inventory in a central repository	Inventory, classification and update of assets is done completely in automatic mode, allowing to manage the entire lifecycle of an asset (identification, assignment, status changes, removal, etc.)
	ID.AM-2: Software platforms and applications within the organization are inventoried	Table 6.1: Assets identification (IA)	See ID.AM-1	See ID.AM-1	See ID.AM-1
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Table 6.2: Responsibility assignment (AR)	The Company Owner and/or the Top Management designates the representative for Cyber Security, formally defining its tasks. They also establish technical specifications for an adequate use of information and IT tools by all involved parties (e.g. employee, consultants, third	A Company Policy document for the Cyber Security defining and clearly formalizing roles, responsibilities and activities required to all involved parties, clearly communicating to them the commitment of the Owner and of the Company Top Management with respect	N/A



Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cyber Security National Lab

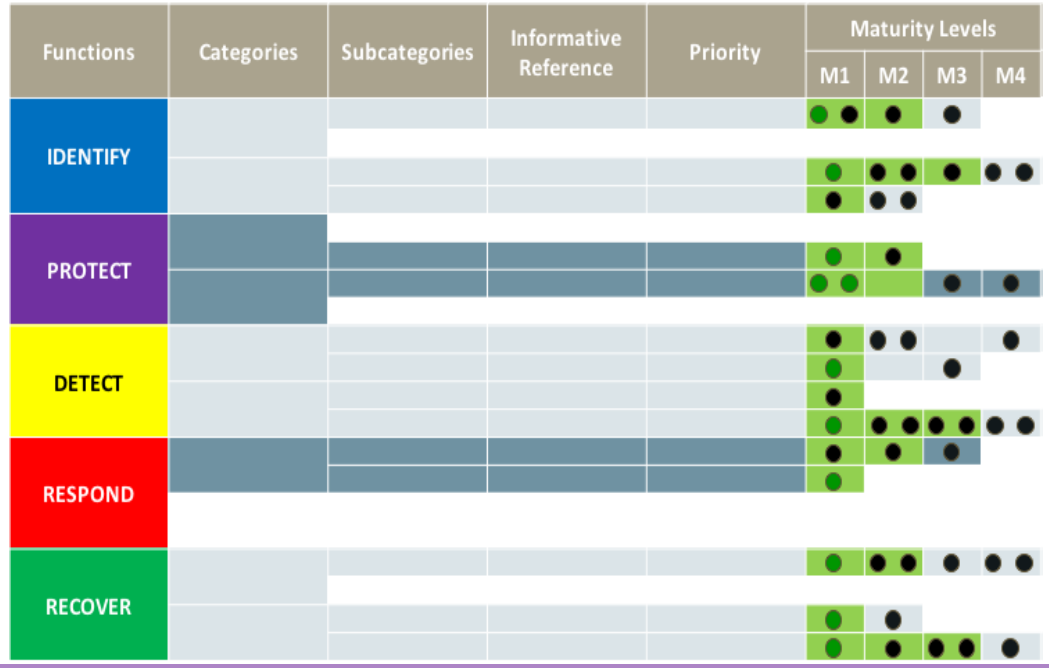
Contextualization

The National Framework can be «customized» so as to adapt it to a specific context (e.g. sectors, public administrations, organizations)

Contextualization

The Framework can be adapted to a specific scenario through a Contextualization:

- Selection of Subcategories
- Definition of the Priority Level for each selected Subcategory
- Definition of the Maturity Levels and…



of the Controls to reach them

Given a Contextualization, it is possible to define:

- The Current Profile

  The "as is" state

- A Target Profile

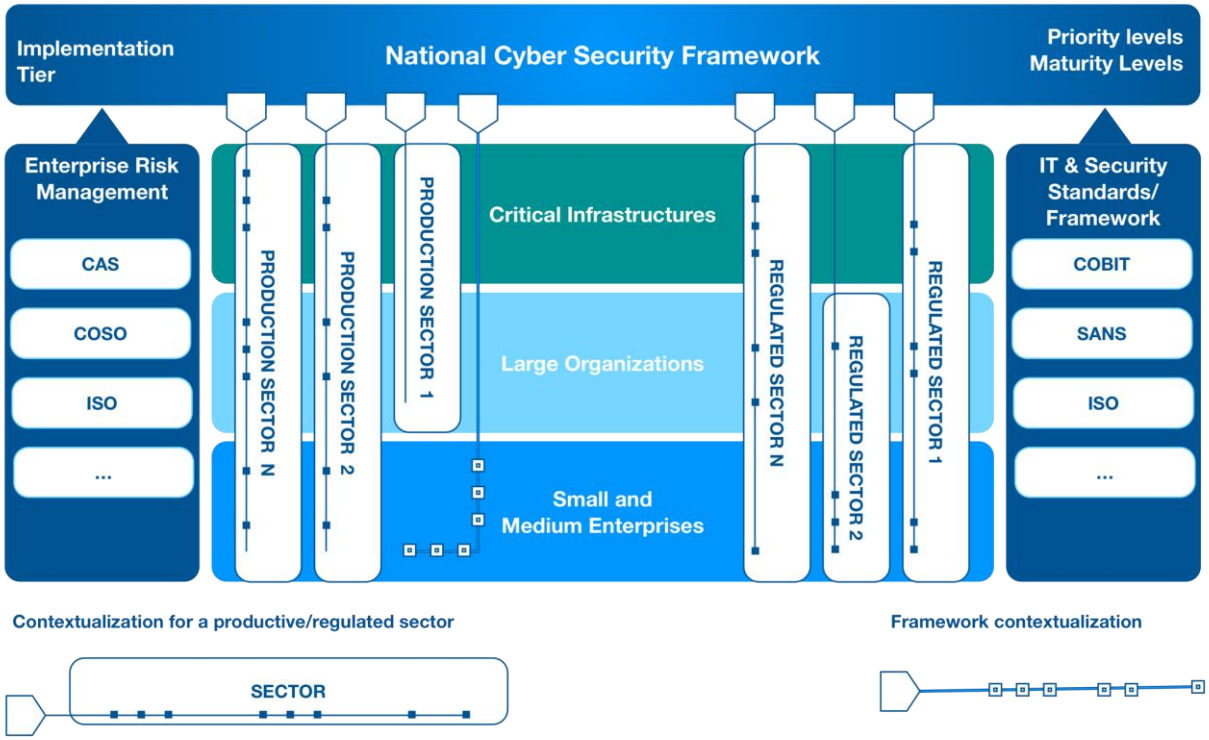
  The "to be" state

Contextualization

A contextualization can be defined for

- A single organization
- An entire economic/productive sector
- Groups of organizations based on scale (e.g. SME, Large Enterprises)
- Organizations belonging to regulated sectors (e.g. PAs, banks, …)
- Critical Infrastructures
- …

Contextualization



Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cyber Security National Lab

Framework 2.0

- Integration in the core of the new subcategories of the NIST CSF version 1.1

Framework NIST 1.0

- 5 function
- 22 category
- 98 subcategory

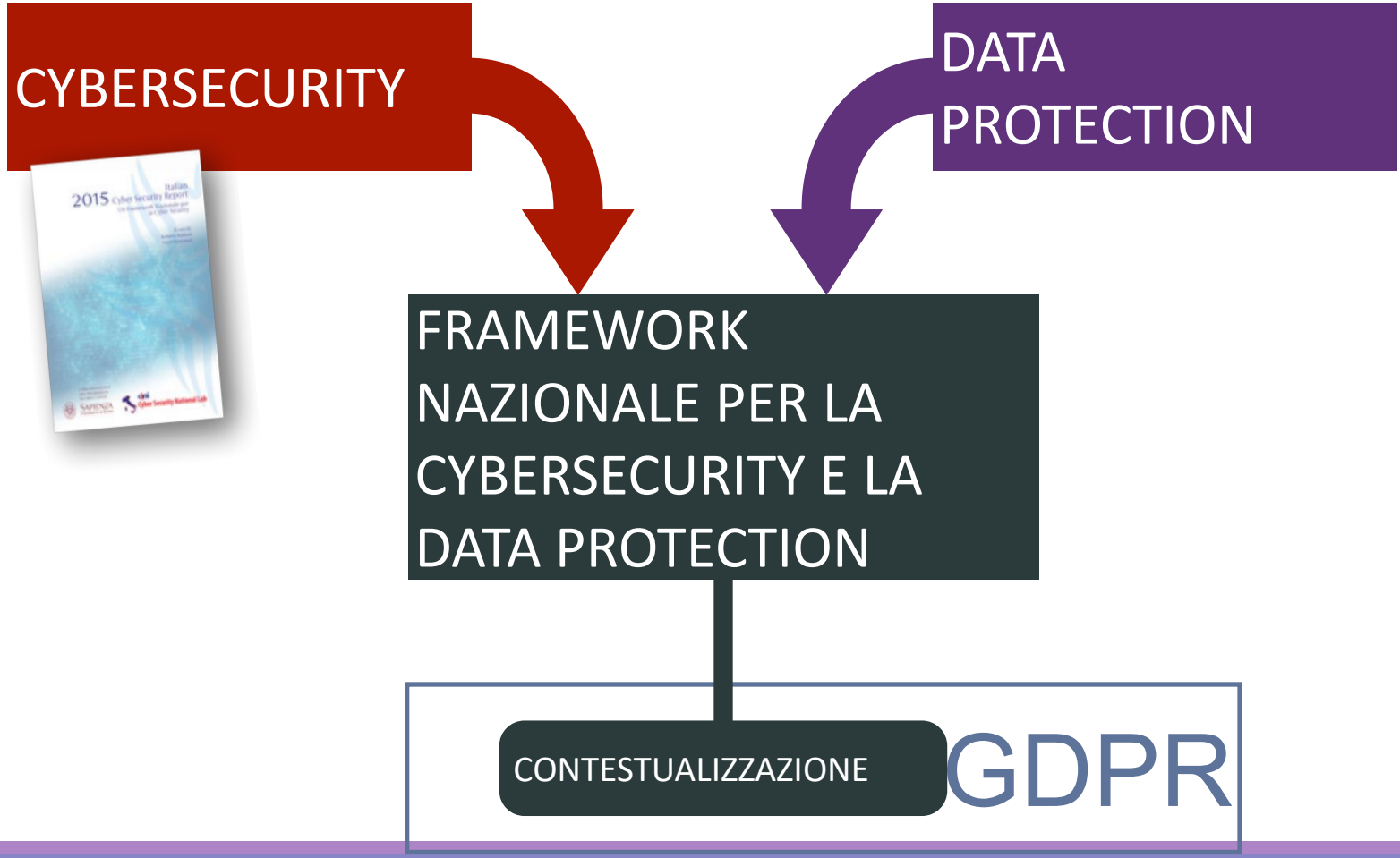
Framework NIST 1.1

- 61 improvements
- 17 on the framework core
- +1 category (supply chain)
- +10 subcategory

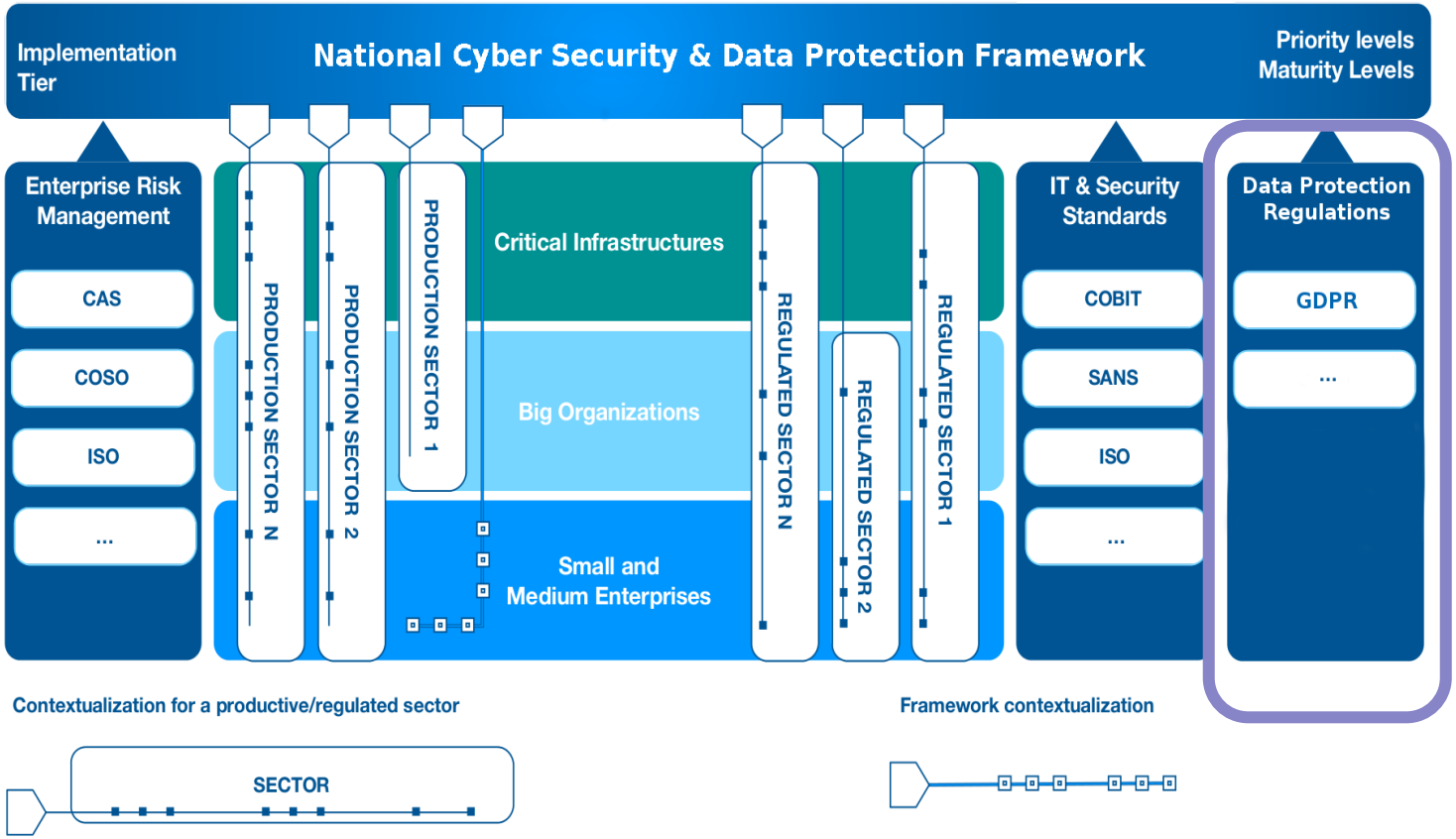
PR.DS-1: I dati e le informazioni memorizzate sono protette

PR.DS-5: Protections against data leaks are implemented

Framework 2.0



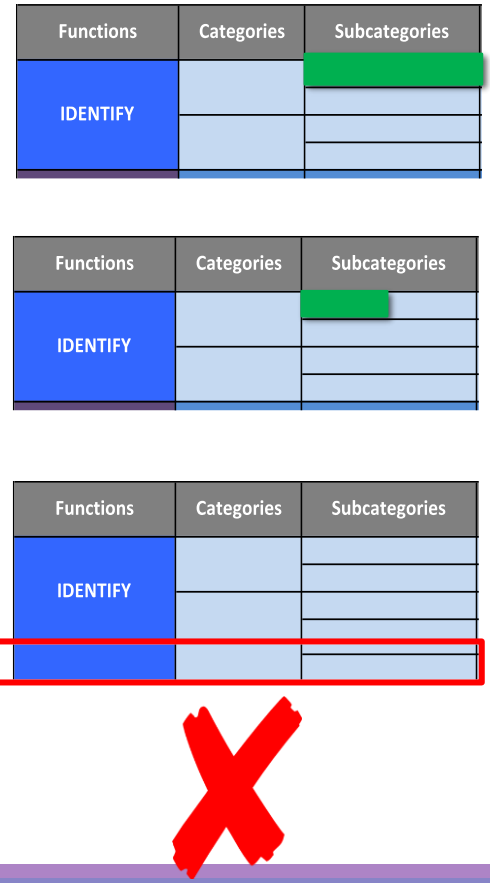
Framework for CS & DP



Mapping Data Protection - Framework

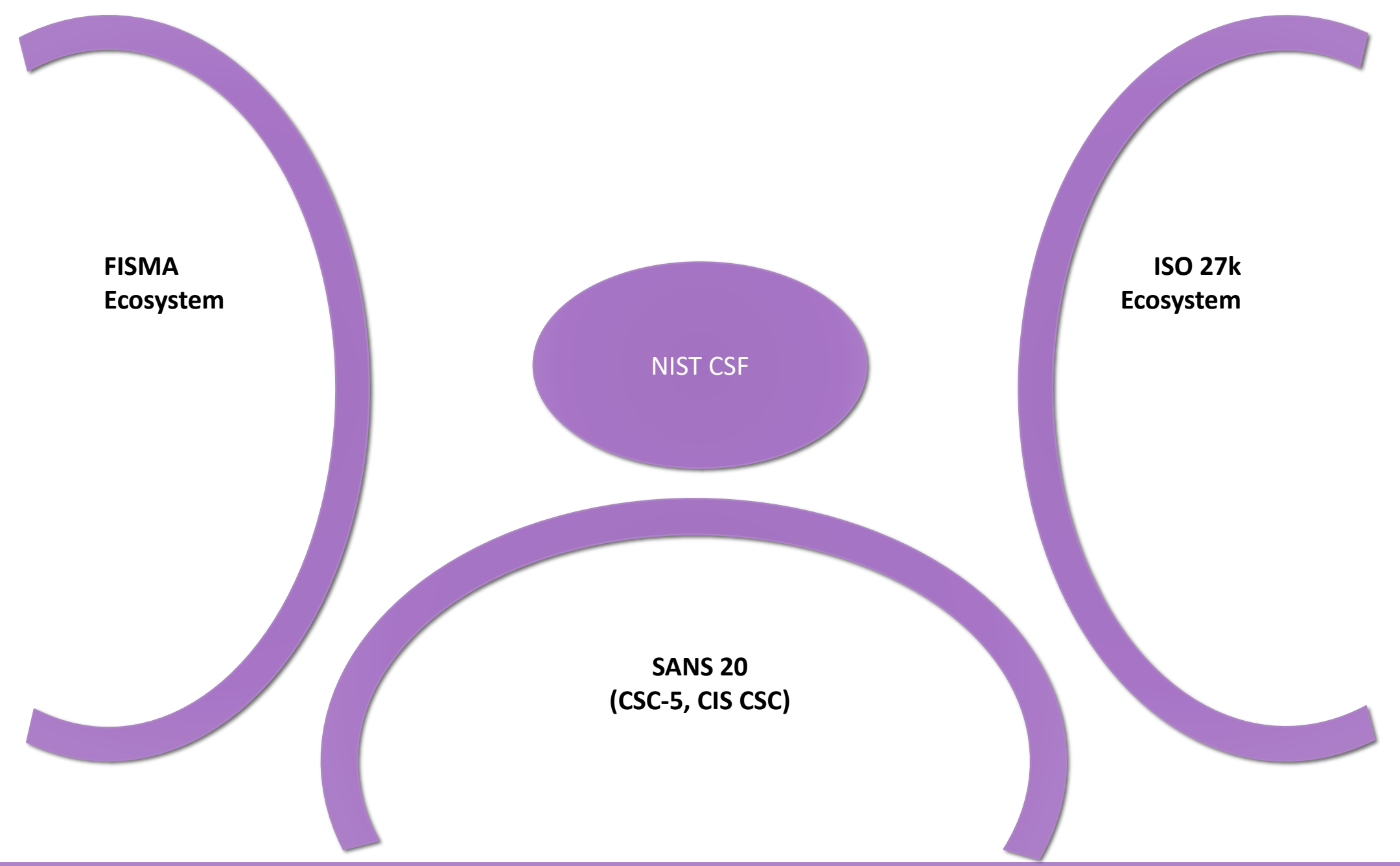
4 possible cases

1. Perfect placement
    1. On 1 single subcategory
    2. On more than one subcategory
2. Partial placement
    1. On 1 single subcategory
    2. On more than one subcategory
3. Not possible placement
    1. Needs for a new subcategory
4. Not needed placement



A COMPARISON OF CSF

A Special thanks to Ing. Luca Montanari for some of the following slides


FISMA
Ecosystem
NIST CSF
ISO 27k
Ecosystem
SANS 20
(CSC-5, CIS CSC)

FISMA Ecosystem

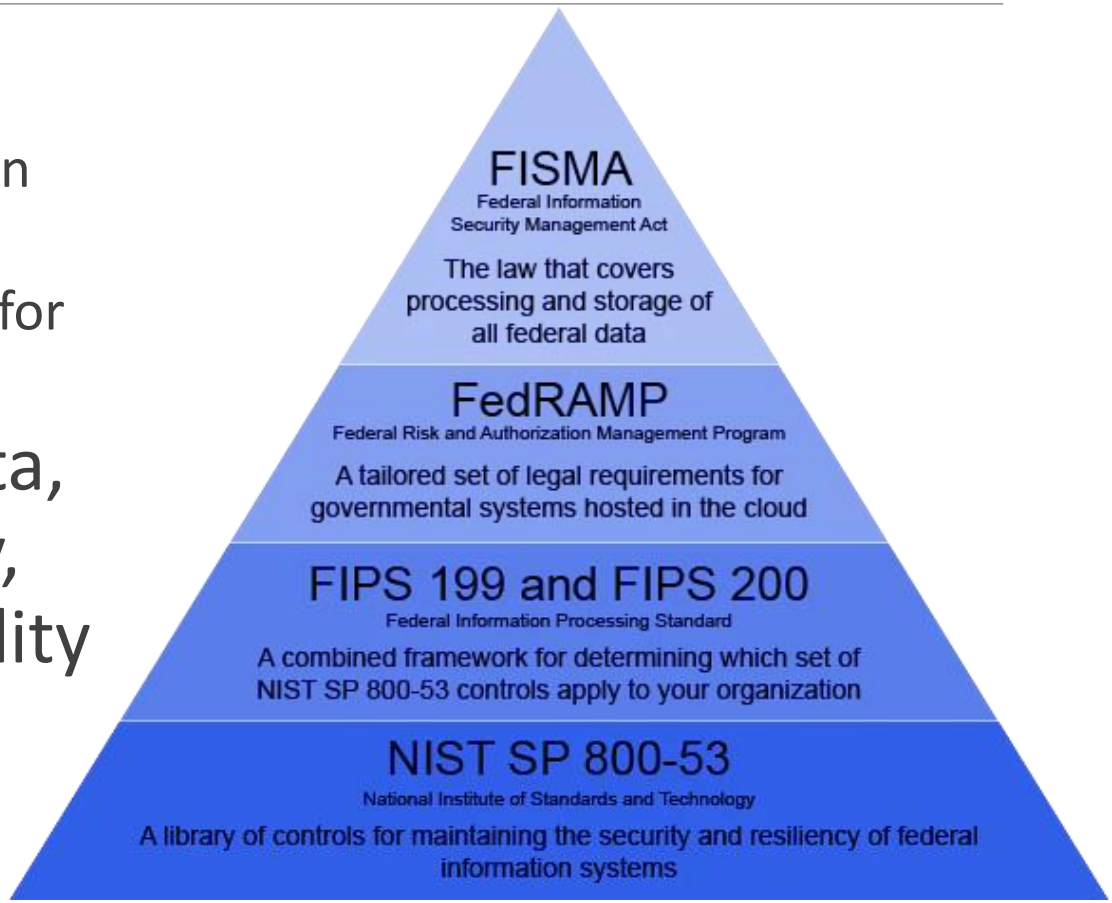
2002, USA.

USA President signs the E-government Act where in Title III "**F**ederal **I**nformation **S**ystem **M**anagement **A**ct" requires that:

> ***each federal agency*** *develops, documents and implements an agency-wide program to provide* ***information security*** *to all information and information systems that support assets and agency processes,* ***including those provided or managed by other agencies****, contractors or third parties*

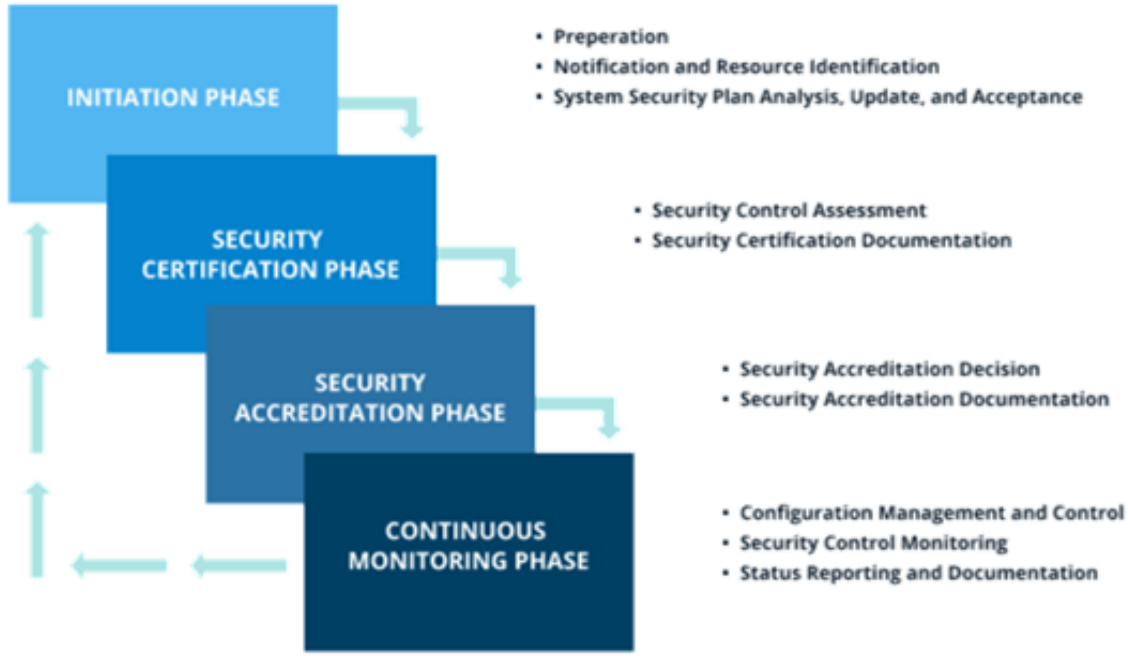
Introduction to FISMA

- Overview of FISMA:
  - Enacted in 2002, amended in 2014
  - Mandates security controls for federal information systems
- Objective: Protect data, ensure confidentiality, integrity, and availability



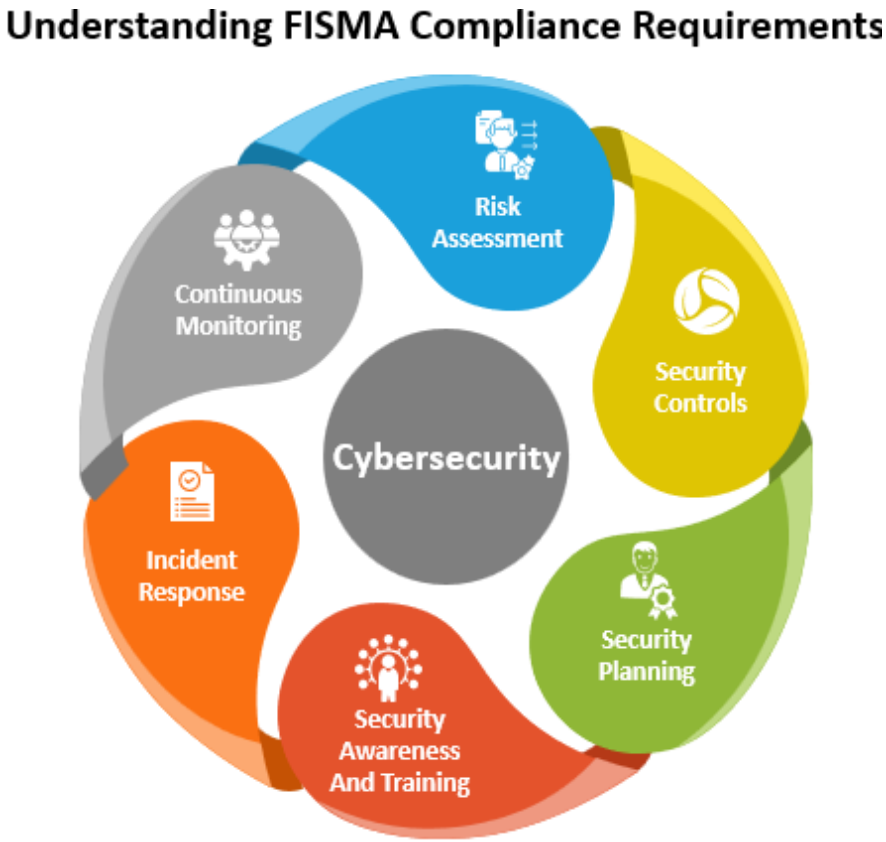
Importance of FISMA Compliance

- why FISMA matters:
  - federal requirement for agencies and contractors
  - reduces risk of data breaches and cyber threats
- consequences of non-compliance:
  - legal penalties
  - reputational damage
  - operational disruptions



FISMA Ecosystem Overview

- ecosystem components:
  - information systems, networks, data, devices
  - users and third-party providers
- goal: establish a secure environment across all components



Mapping FISMA ecosystem to CSF

FISMA Ecosystem Element	Mapped CSF Function	Explanation
Risk Assessment	Identify	Determines critical assets, categorizes systems (FIPS 199), and assesses risks.
Security Planning	Identify + Protect	System Security Plan (SSP) documents how protections are applied.
Security Controls	Protect	Implementation of safeguards from NIST SP 800-53 (access control, encryption, audit, etc.).
Security Awareness & Training	Protect	Human element of protection: educating users to prevent mistakes/insider threats.
Incident Response	Respond + Recover	Procedures to handle incidents and resume operations.

Key Phases of FISMA Implementation

1. Risk Assessment & Planning
2. Selection of Security Controls
3. Implementation of Controls
4. Continuous Monitoring
5. Certification & Accreditation
6. Incident Response
7. Ongoing Reporting & Documentation

FISMA Ecosystem Implementation Project

Phase 1: Standards and Guidelines Development (2003-2012+)

Phase 2: Implementation and Assessments Aids

Documents 1

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems (Final)

FIPS Publication 200, Minimum Security Requirements for Federal Information and Federal Information Systems (Final)

NIST Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems (Final)

NIST Special Publication 800-30 Revision 1, Risk Management Guide for Information Technology Systems (Final)

NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Final)

NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View (Final)

Documents 2

NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (Final)

NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations (Final)

NIST Special Publication 800-53A Revision 1, Guide for **Assessing the Security Controls** in Federal Information Systems and Organizations, Building Effective Security Assessment Plans (Final)

NIST Special Publication 800-59, Guide for Identifying an Information System as a National Security System (Final)

NIST Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories (Final)

NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems (Final)

NIST Special Publication 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations (Final)

FIPS 199 & FIPS 200

Two documents with less than 10 pages each:

- FIPS 200: “Minimum Security Requirements for Federal Information and Information Systems”
  - all agencies owning federal data must have their information systems certified according to 800-53 with low, moderate and high profiles compared to baseline 800-53
- FIPS 199: “Standards for Security Categorization of Federal Information and Information Systems”
  - Defines the potential impact on organizations and individuals in case of confidentiality, integrity, or availability loss (3 levels)

The *potential impact* is **LOW** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[2]

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The *potential impact* is **MODERATE** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The *potential impact* is **HIGH** if—

– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

SP 800-53

Follows directly from FIPS 199 e 200

Last version is Revision 5 released in September 2020

Aims:

1. Provide a security and privacy controls catalogue for federal organizations and information systems

2. Provide a process to select controls to protect *Mission, functions, image, reputation, assets, individuals, State* from cyber attacks, disasters, malfunctions and human errors

3. Provide a methodology for selecting critical controls (baseline)

SP800-53

Structure and content:

- ~ 460 pages
  - 3 main chapters
  - 10 appendixes

Controls are organized in 18 families

Table of Contents

SP800-53

For ease of use in the security control selection and specification process, controls are organized into eighteen families.

- Each family contains security controls related to the general security topic of the family.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

SP800-53

Security Control Structure

Section	Description
Control	prescribes specific security-related activities or actions to be carried out by organizations or by information systems
Supplemental guidance	provides non-prescriptive, additional information for a specific security control.
Control enhancements	provides statements of security capability to: (i) add functionality/specificity to a control; and/or (ii) increase the strength of a control.
References	includes a list of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines that are relevant to a particular security control
Priority and baseline allocation	Provides (i) the recommended priority codes used for sequencing decisions during implementation and (ii) the initial allocation of security controls and control enhancements to the baselines

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full-text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

SP 800-53 Security Control Example

SP 800-53

SECURITY CONTROL BASELINES

- **Aim**: To assist organizations in making the appropriate selection of security controls for information systems
- **Baseline controls**
  - Are the starting point for the security control selection process (as described in the document) and
  - Are chosen based on the security category and associated impact level of information systems (determined in accordance with FIPS Publication 199 and FIPS Publication 200)

- Three security control baselines have been identified corresponding to the *low-impact*, *moderate-impact*, and *high-impact* information systems

SP 800-53

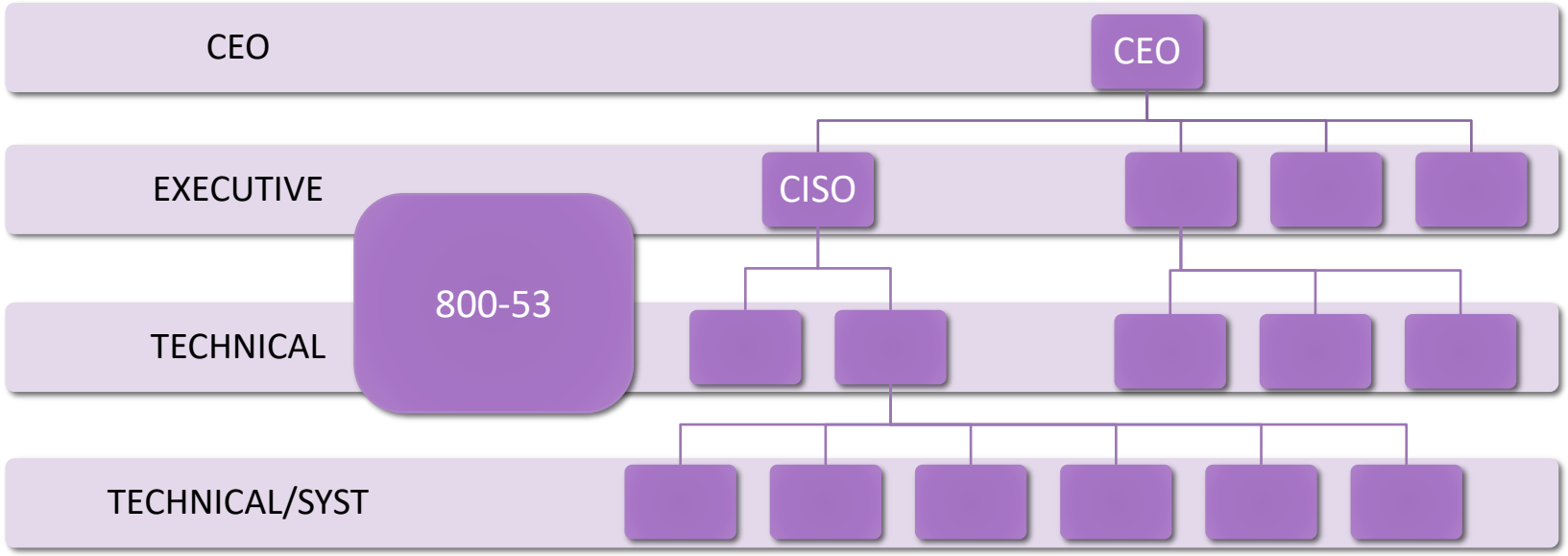
Limitations:

Tied to the concept of federal information systems, to the US Legislation and EOs, POLICIES, DIRECTIVES, INSTRUCTIONS, REGULATIONS, AND MEMORANDA, all US (over 50 in total)

Very complex and oriented to operational people

Certifiable outside the USA!?!

Target audience



ISO 27k

ISO/IEC 27000 — Information security management systems — **Overview and vocabulary**

ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems - **Requirements**

ISO/IEC 27002 — Code of practice for information security management

ISO/IEC 27003 — Information security management system **implementation guidance**

ISO/IEC 27004 — Information security management — Measurement

ISO/IEC 27005 — Information security risk management

ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on the management system)

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on the information security controls)

ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014 — Information security governance.[4] Mahncke assessed this standard in the context of Australian e-health.[5]

ISO/IEC TR 27015 — Information security management guidelines for financial services

ISO 27k

ISO/IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032 — Guideline for cybersecurity

ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts

ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

ISO/IEC 27033-4 — Network security - Part 4: Securing communications between networks using security gateways

ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security

ISO/IEC 27035 — Information security incident management

ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

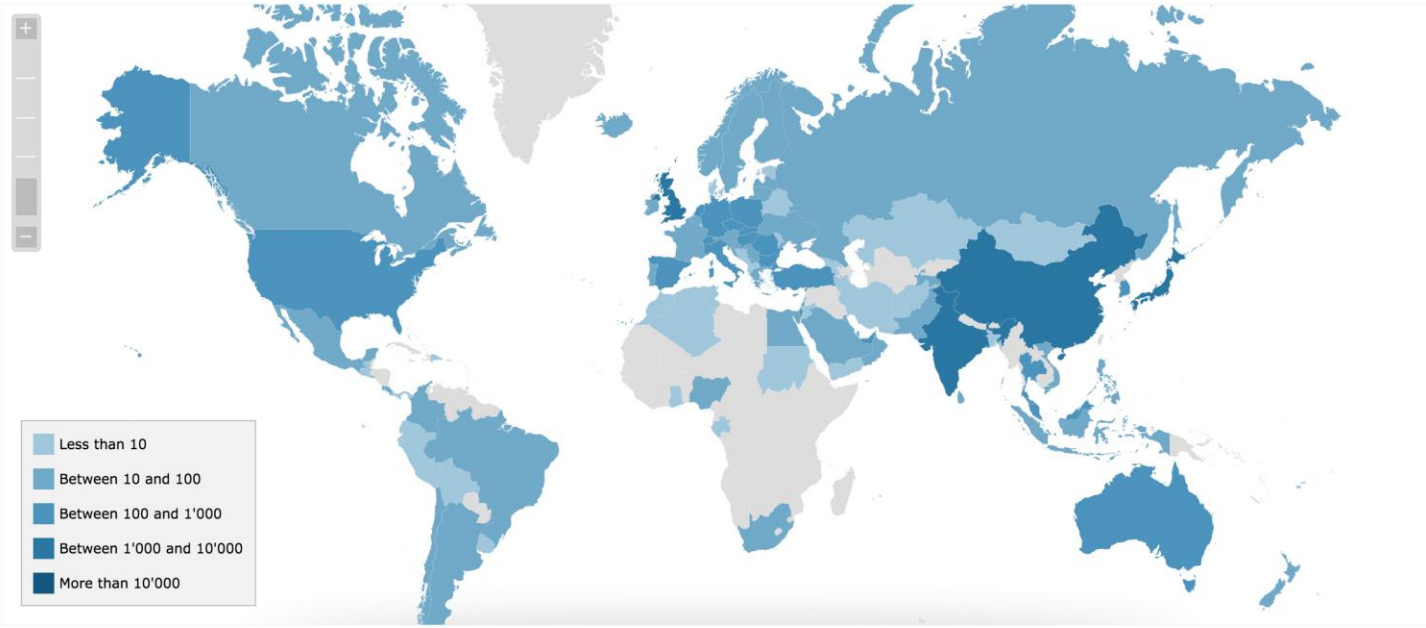
ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO 27799 — Information security management in health using ISO/IEC 27002. The purpose of ISO 27799 is to provide guidance to health organizations and other holders of personal health information on how to protect such information via implementation of ISO/IEC 27002.

ISO 27001 and 27002

It is the most international framework, recognized in over 60 countries.

http://wv
survey.ht

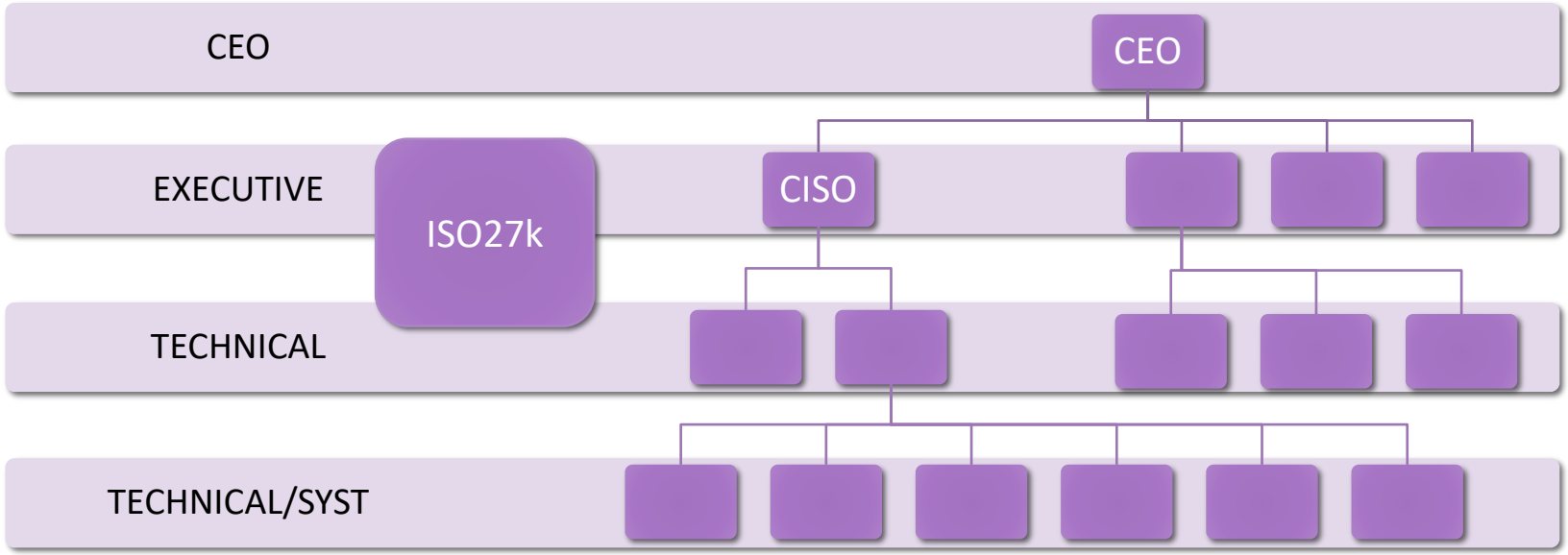


ISO 27k

Limitations:

- It is expensive and therefore it is rare to see SMEs adopting the standard
- Managing an ISMS is complex and requires a specific office
- It does not define any priority between controls
- All requirements are mandatory
- It is voluntary

TECHNICAL vs EXECUTIVE LEVEL



ISO/IEC 27k vs NIST SP 800-53

The 800-53 has an appendix that provides the mapping between the controls of the two standards

All FISMA standards are very "system-oriented" while ISOs are dedicated to the organization

- The FISMA certification is for "IT-System" while for the ISO it is for "management System"

"Both result of hundreds of years man of experts"

CIS controls

What is CIS?

- The **Center for Internet Security** is a USA non-profit organization focused on improving global cybersecurity standards and practices.
- CIS works with various experts from industry, government, and academia to develop best practices and guidelines that help organizations secure their IT systems and data against cyber threats.

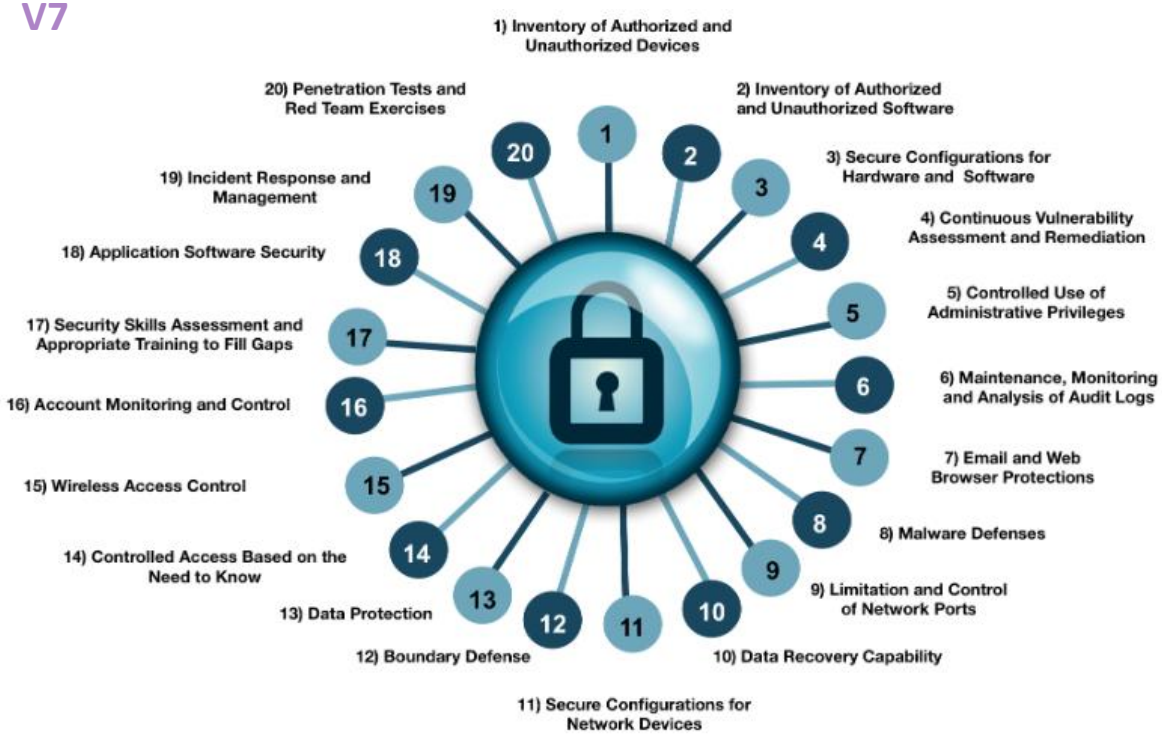
What are CIS Controls?

- a prioritized set of actions designed to help organizations strengthen their cybersecurity posture.
- developed by a global community of cybersecurity experts and provide clear, actionable steps to protect against the most prevalent cyber threats.
- organized into different categories and ranked based on effectiveness and ease of implementation, making them highly practical for organizations of all sizes.

CIS Controls Overview

- set of best practices for securing IT systems and data
- developed by the Center for Internet Security (CIS)
- prioritized actions to defend against common cyber threats

V7



Categories of CIS Controls

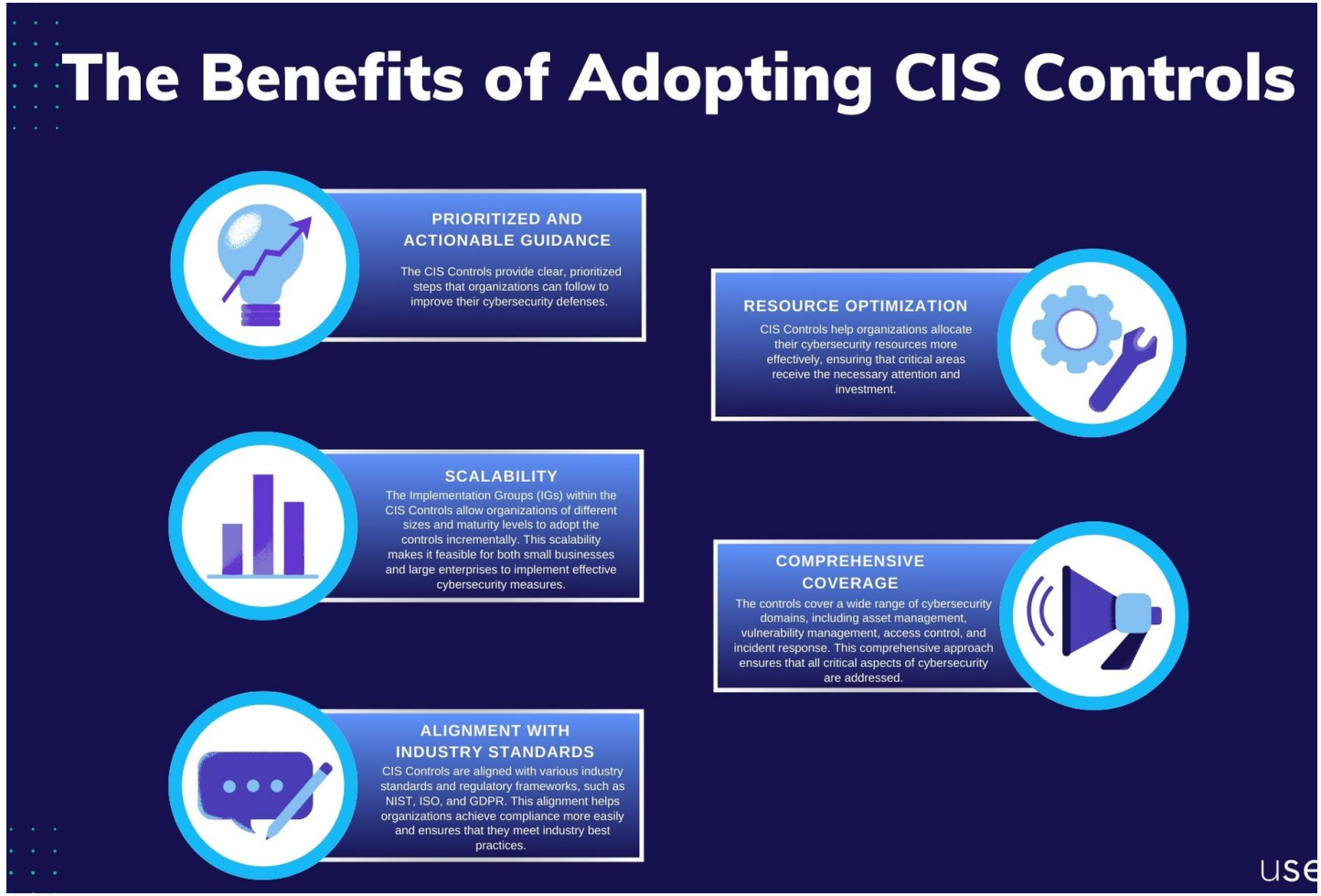
- Basic Controls (1–6): Fundamental cybersecurity measures
- Foundational Controls (7–16): Advanced security practices
- Organizational Controls (17–18): Policies and processes for security.

Top 6 Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Admin Privileges
5. Configuration for Hardware and Software on Mobile Devices, Laptops and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Benefits of CIS Controls

- Effective defense against common attack vectors.
- Easy to implement, even with limited resources.
- Complementary to other security frameworks (e.g., NIST, ISO).
- Provides measurable practices for continuous improvement.



OVERVIEW

	NIST SP 800-53	ISO 27001	CIS Control	NIST CSF
Last update	Revision 5 2020	2022 amended in 2024 (climate change)	version 8 released in May 2021	version 2.0 released in 2023
Size	Large	Medium	Medium	Small
Complexity	High	Medium	Medium	Low
International spreading	No	Yes	Yes	Medium
Target organizational level	Operational	Operational	Tactical/ Operational	Strategical
Certifiability	Yes	Yes	No	No
Is it mandatory?	Yes in USA	No	No	No
Cost	-	High	Low	Low