Cybersecurity Framework

Luca G. Carbone

Tutorial Days CCR 10-12/10/2022 – LNF

Cybersecurity Framework

CYBEREXPERTS.com Cybersecurity Cybersecurity Guides Cybersecurity Encyclopedia Contact Us

23 Top Cybersecurity Frameworks

International Organization for St...
ISO
27001

CIS®

CIS Critical Security Controls

COBIT
GOVERNANCE, CONTROL and ASSURANCE for INFORMATION and RELATED TECHNOLOGY

AgID Basic Security Controls

NIST SP 800-53 Revision 5

NIST Security and Privacy Controls for Federal Information Systems and Organizations

Cybersecurity Framework

- Strumento operativo per **organizzare riproducibilmente** le attività fondamentali della cybersecurity:
  - gestione del rischio
  - protezione delle risorse aziendali
  - protezione dei dati (sensibili, strategici, ...)
  - gestione accessi
  - …

Schema logico costituito da processi, buone pratiche e tecnologie per sviluppare programmi di cybersecurity efficienti.

Misure Minime AgID

Tipologia	Descrizione
ABSC1 (CSC1)	INVENTARIO DEI DISPOSITIVI AUTORIZZATI
ABSC2 (CSC2)	INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC3 (CSC3)	PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC4 (CSC4)	VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
ABSC5 (CSC5)	USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC8 (CSC8)	DIFESE CONTRO I MALWARE
ABSC10 (CSC10)	COPIE DI SICUREZZA
ABSC13 (CSC13)	PROTEZIONE DEI DATI

IDENTIFY

PROTECT

CIS Critical Security Controls V8

1 - Inventory and Control of Enterprise Assets	10 – Malware Defenses
2 - Inventory and Control of Software Assets	11 – Data Recovery
3 – Data Protection	12 – Network Infrastructure Management
4 - Secure Configuration of Assets and Software	13 – Network Monitoring and Defense
5 – Account Management	14 – Security Awareness and Skill Training
6 – Access Control Management	15 – Service Provider Management
7 – Continuous Vulnerability Management	16 – Application Software Security
8 – Audit Log Management	17 – Incident Response Management
9 – Email and Web Browser Protection	18 – Penetration Testing

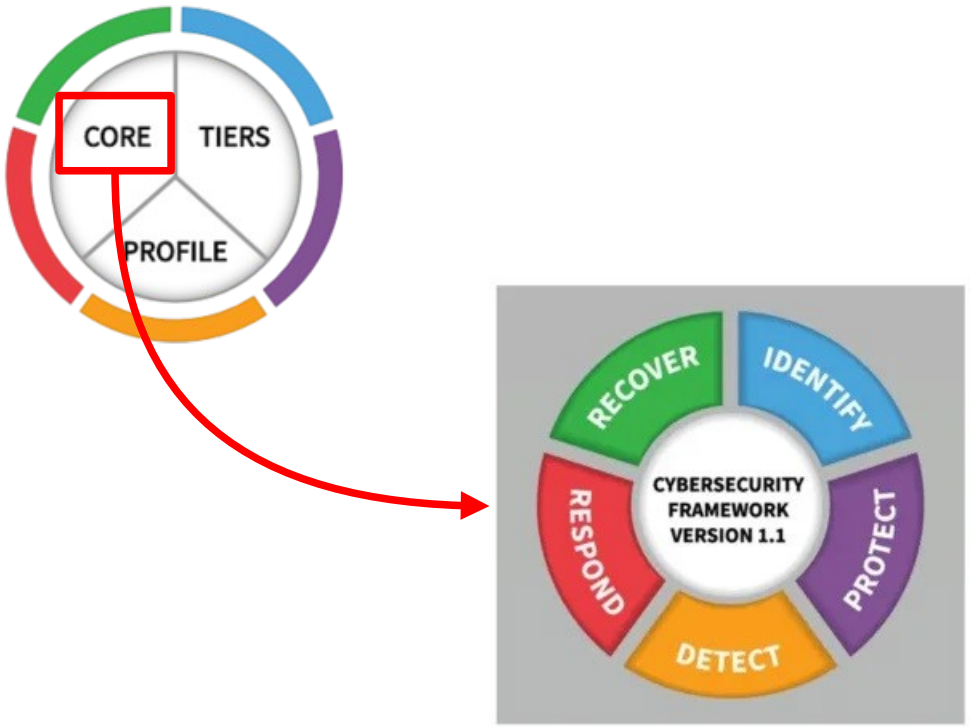
Control 01: Inventory and Control of Enterprise Assets

Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
1.1	**Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Devices	Identify	●	●	●
1.2	**Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Devices	Respond	●	●	●
1.3	**Utilize an Active Discovery Tool** Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.	Devices	Detect		●	●
1.4	**Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory** Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Devices	Identify		●	●
1.5	**Use a Passive Asset Discovery Tool** Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Devices	Detect			●

NIST Cybersecurity Framework

The Framework is a *voluntary* guidance, based on existing standards, guidelines, and practices for organizations to better *manage and reduce cybersecurity risk.* In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.



Framework attributes

Principles of Current and Future Versions of the Framework

- Establishes a common and accessible language
  - Describes desired outcomes
  - Understandable by everyone
  - Applies to any type of risk management
  - Defines the entire breadth of cybersecurity
  - Spans both prevention and reaction
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

CORE: functions

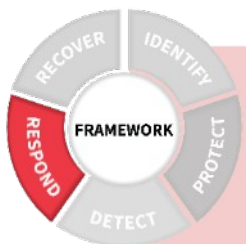
IDENTIFY

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

Five **key** functions: … provide a comprehensive view of the lifecycle for managing cybersecurity over time.

PROTECT

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



RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

DETECT

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

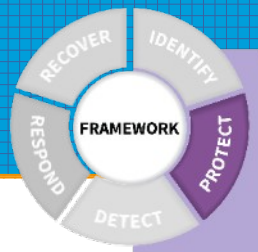
RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

IDENTIFY

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

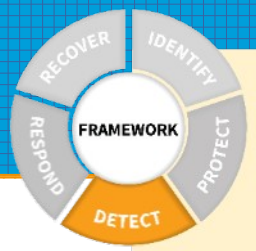
- **Identify critical enterprise processes and assets**
- **Document information flows**
- **Maintain hardware and software inventory**
- **Establish policies for cybersecurity that include roles and responsibilities**
- **Identify threats, vulnerabilities, and risk to assets**



PROTECT

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

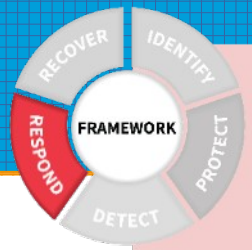
- **Manage access to assets and information**
- **Protect sensitive data**
- **Conduct regular backups**
- **Securely protect your devices**
- **Manage device vulnerabilities**
- **Train users**



DETECT

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

- **Test and update detection processes**
- **Maintain and monitor logs**
- **Know the expected data flows for your enterprise**
- **Understand the impact of cybersecurity events**



RESPOND

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

- **Ensure response plans are tested**
- **Ensure response plans are updated**
- **Coordinate with internal and external stakeholders**

RECOVER

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

- **Communicate with internal and external stakeholders**
- **Ensure recovery plans are updated**
- **Manage public relations and company reputation**

CORE: categories

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

The Categories were designed to cover the breadth of cybersecurity objectives for an organization, while not being overly detailed. It covers topics across **cyber, physical, and personnel**, with a focus on business outcomes.

CORE: subcategories

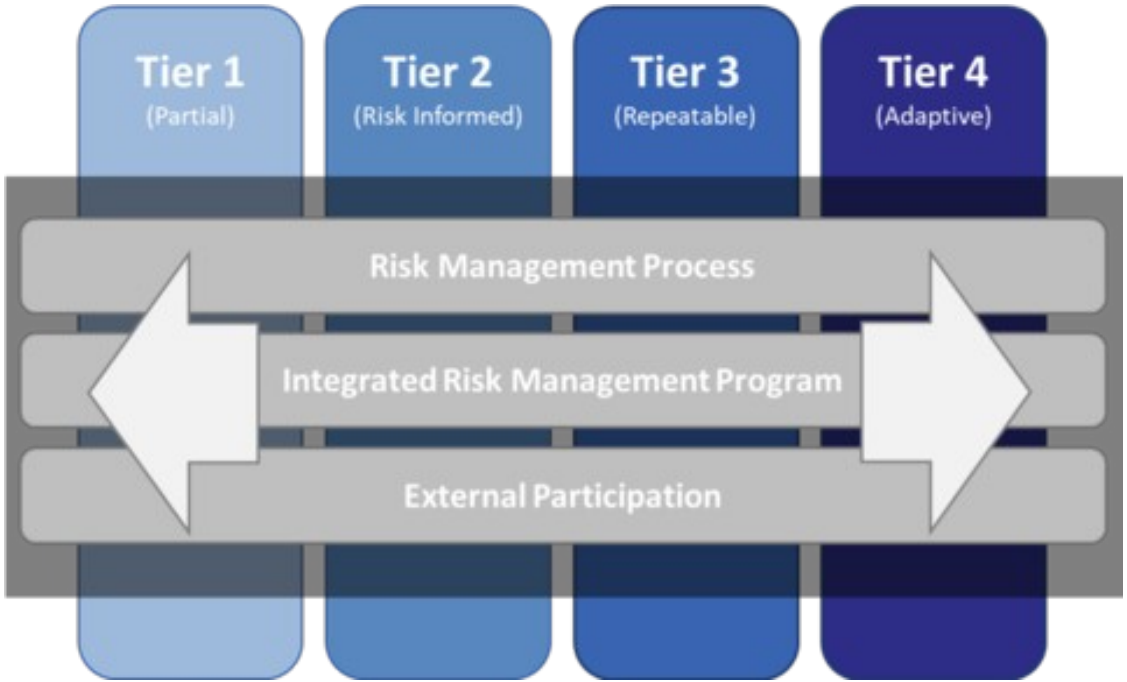
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information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

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

There are 108 Subcategories, which are outcome-driven statements that provide considerations for creating or improving a cybersecurity program. Because the Framework is outcome driven and does not mandate how an organization must achieve those outcomes, it *enables risk-based implementations that are customized to the organization's needs*.

CORE: implementation tiers

***ad-hoc* risk management processes**
limited cyber risk awareness

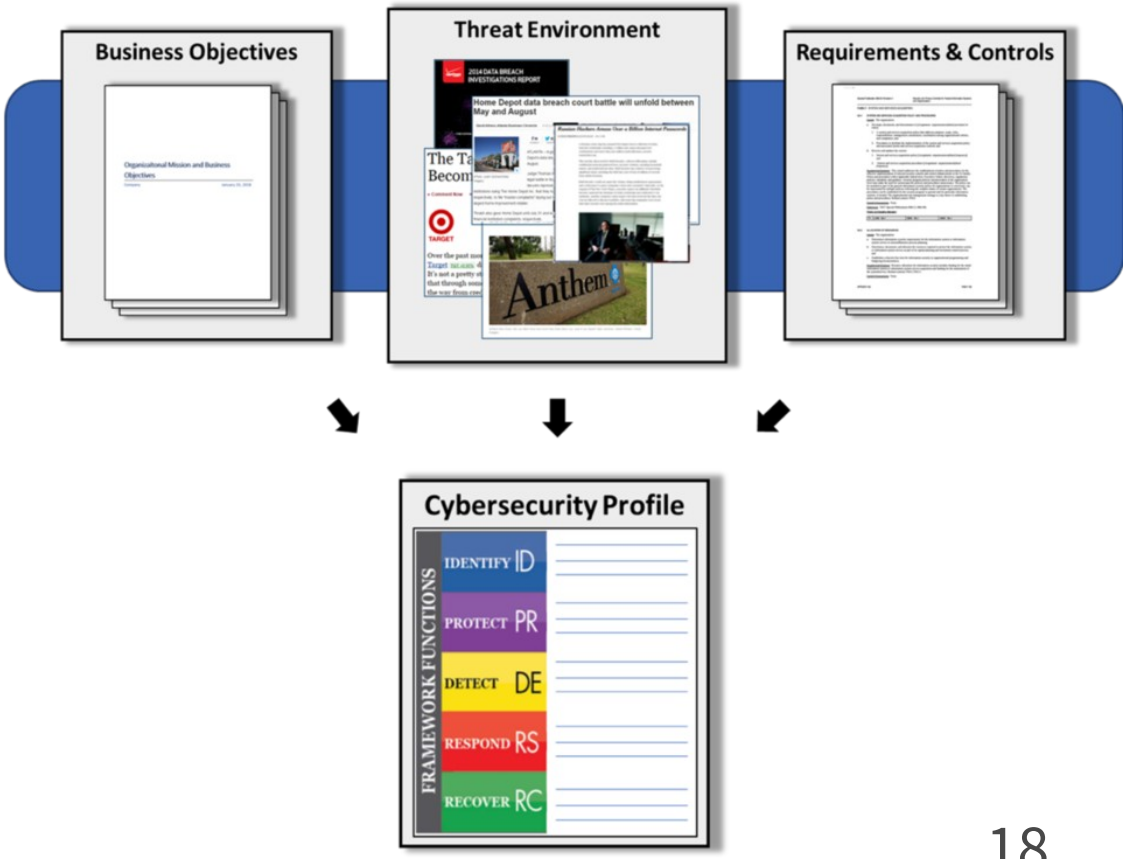


continuous improvement
adapt to changing threats

The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor, and how well integrated cybersecurity risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity info from external parties. Tiers do not necessarily represent maturity levels. Organizations should determine the desired Tier, ensuring that the selected level meets organizational goals, reduces cybersecurity risk to levels acceptable to the organization, and is feasible to implement, fiscally and otherwise.

CORE: profiles

Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile with a "Target" Profile. Profiles are about optimizing the Cybersecurity Framework to best serve the organization. The Framework is voluntary, so there is no 'right' or 'wrong' way to do it.



CORE: profiles

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

One way of approaching profiles is for an organization to map their cybersecurity requirements, mission objectives, and operating methodologies, along with current practices against the subcategories of the Framework Core to create a Current-State Profile and a Target Profile to allow Gap Analysis and create a prioritized implementation map .

Framework Nazionale per la Cybersecurity e la Data Protection

Novità in Framework 2.0

- Allineamento alla versione 1.1 del NIST CSF
- Aggiornamento Core - introduzione 1 Category & 9 Subcategory relative alla Data Protecton (e relativi controlli di sicurezza che implementano effettivamente le attività);
- Arricchimento Riferimenti Informativi UE/IT (GDPR, MM AgID, direttiva NIS)
- Adattamento a contesto nazionale (flessibilità: PMI, ...):
  - Livelli di priorità (già previsti in NIST CSF ma meno formalizzati)
  - Livelli di maturità
  - Contestualizzazioni

Esempio: Asset Management

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· **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 · **Misure Minime AgID** ABSC 1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· **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 · **Misure Minime AgID** ABSC 2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	· **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 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1

MM

Livelli di priorità

- Associati alle subcategory
- Possibilità di definire scala personalizzata – scala suggerita:
  - **ALTA**: permettono di ridurre sensibilmente il rischio. Vanno implementate indipendentemente dalla difficoltà realizzativa.
  - **MEDIA**: permettono di ridurre il rischio e risultano di semplice implementazione.
  - **BASSA**: permettono di ridurre il rischio ma risultano di difficile implementazione.
- *Formalizzano* gap analysis e prioritizzazione roadmap

Livelli di maturità

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA	Il censimento, la classificazione e l'aggiornamento degli asset (intesi come informazioni, applicazioni, sistemi ed apparati presenti) avviene in modalità per lo più manuale secondo un processo definito e controllato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema parzialmente automatico, che consenta di automatizzare almeno la fase di "discovery" dei sistemi connessi in rete, rilevando le principali caratteristiche degli stessi (caratteristiche hardware, software installati, configurazioni adottate, ecc.) e registrando l'inventario ottenuto in un repository centralizzato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema completamente automatico, che consenta di gestire l'intero ciclo di vita di un asset (identificazione, assegnazione, cambiamenti di stato, dismissioni)
	ID.AM-2: Sono censite le	Tabella 6.1:	Vedi ID.AM-1	Vedi ID.AM-1	Vedi ID.AM-1

Contestualizzazioni: GDPR

Subcategory	Classe	Priorità	Informative References
DP-ID.AM-7: Sono definiti e resi noti ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	Obbligatoria	ALTA	GDPR - Artt. 24, 26-29, 37-39
DP-ID.AM-8: I trattamenti di dati personali sono identificati e catalogati	Obbligatoria	ALTA	G
DP-ID.DM-4: Sono definiti, implementati e documentati i processi per l'esercizio dei diritti (accesso, rettifica, cancellazione ecc.)	Obbligatoria	ALTA	G
DP-R dati p infor			

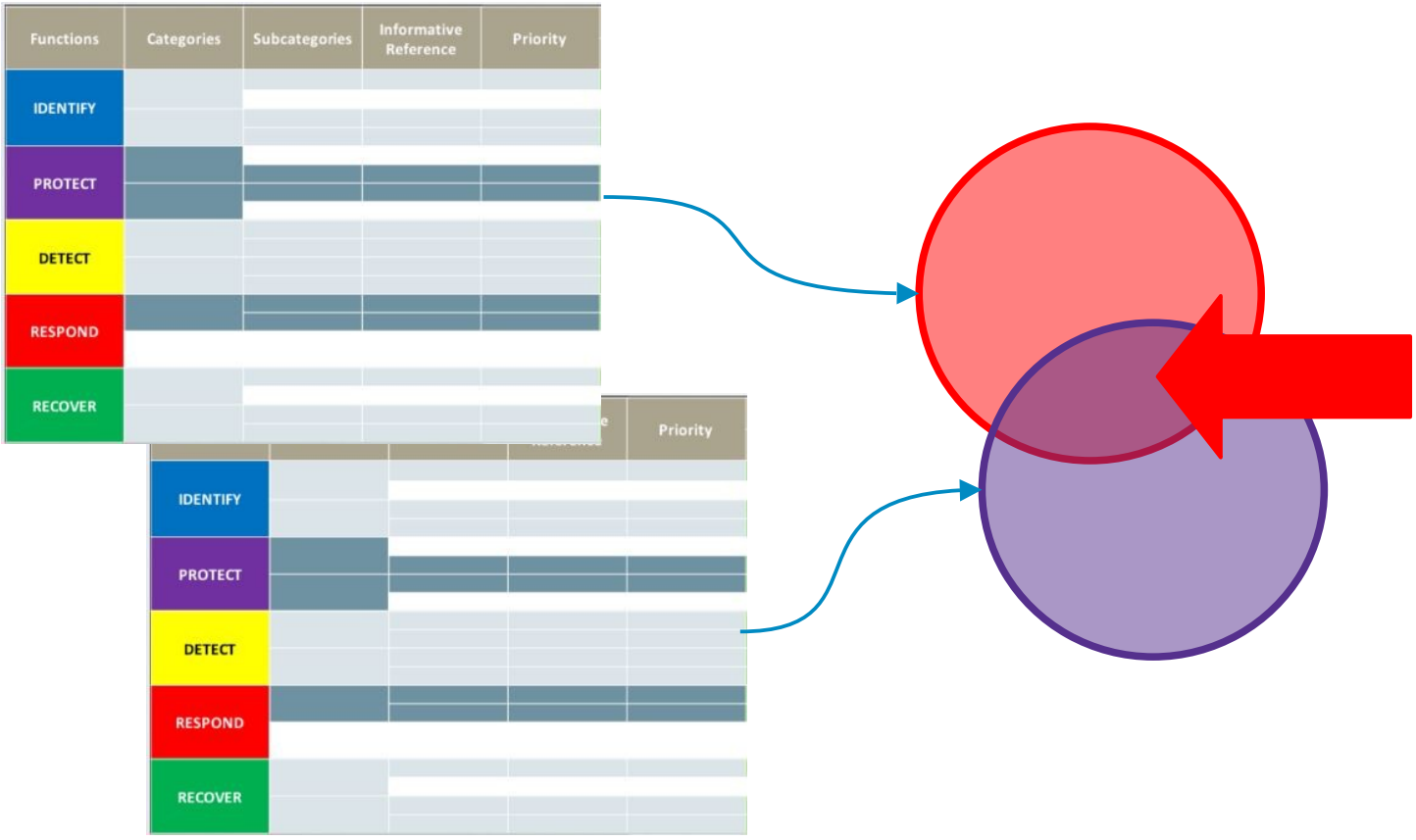
Elementi fondamentali del GDPR

Subcategory	Classe	Priorità
PR.DS-7: Gli ambienti di sviluppo e test sono separati dall'ambiente di produzione	Libera	
DE.CM-8: Vengono svolte scansioni per l'identificazione di vulnerabilità	Libera	
DE.CM-5: Il codice non autorizzato su dispositivi mobili viene rilevato	Libera	

Subcategory	Classe		
PR.AC-4: Gli accessi alle risorse e le autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	Consigli		
PR.DS-4: I sistemi hanno adeguate risorse a disposizione per poter garantire la disponibilità	Consigliata	MEDIA	GDPR – Art. 32
PR.IP-6: I dati sono distrutti in conformità con le policy	Consigliata	ALTA	GDPR - Artt. 5, 17, 32
PR.IP-8: L'efficacia delle tecnologie di protezione viene condivisa	Consigliata	BASSA	GDPR – Art. 32

Elementi non fondamentali, colgono aspetti su cui il GDPR lascia maggiore libertà; possono essere deselezionate in fase di contestualizzazione se non pertinenti

To do: GDPR & MM AgID

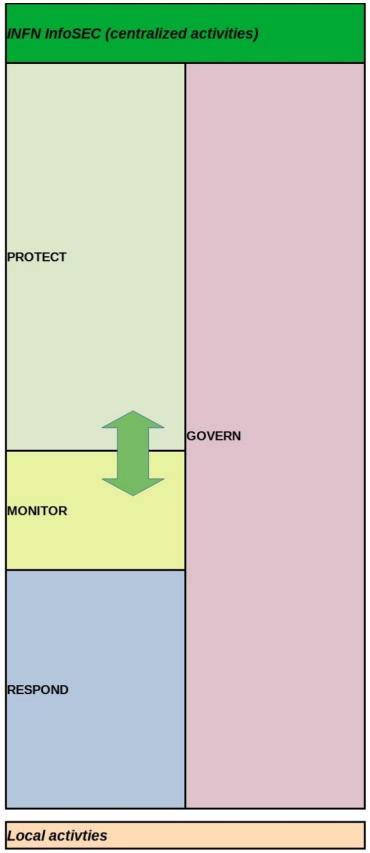


In caso di sovrapposizione (subcategory presenti in entrambe le contestualizzazioni con classe e priorità differenti) vincono:

- Classe superiore
- Priorità maggiore

To do: INFN Sec

Framework	
Function	**Category**
IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
	Data Management
PROTECT	Identity Management, Auth. and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER	Recovery Planning
	Improvements
	Communications



- Replicare struttura e processi di analisi e gestione in > 25 strutture comporterebbe robuste inefficienze, costi alti e problemi di coordinamento;
- Visibilità globale su eventi di sicurezza: tempi di risposta inferiori, diminuita probabilità effetto domino;
- Sfruttamento e trasmissione competenze più efficienti

- Alcune attività puntuali andrebbero comunque svolte localmente nelle sezioni, ma secondo processi definiti e coordinati a livello centrale (asset management, risk assessment, data protection/backup, ...)

Conclusioni

- Il *Framework Nazionale per la Cybersecurity e la Data Protection* è un adattamento al contesto italiano (PMI, PA, …) del CSF del NIST; ne tradisce in qualche modo lo spirito iniziale appesantendolo un po', ma fornisce comunqe uno schema organizzativo del quale potremmo certamente beneficiare: ***SE*** decideremo di implementarlo sarà comunque necessario un certo lavoro propedeutico di contestualizzazione alla realtà INFN.
- A settembre 2021 è stata pubblicata la versione 1.0 de la *Metodologia per il cybersecurity assessment con il Framework Nazionale*: ne parleremo (forse già a inizio 2023).

Il Framework Nazionale è un prodotto del **CIS** - *Centro di Ricerca di Cyber Intelligence and Information Security* della Sapienza, fondato da Roberto Baldoni e da quest'ultimo diretto per 5 anni. Baldoni è attualmente Direttore Generale di **ACN** – *Agenzia per la Cybersicurezza Nazionale*, organismo che pubblica la **Strategia Nazionale di Cybersicurezza** e il relativo **Piano di Implementazione…**

Misura #11

Porre in essere iniziative di sensibilizzazione per favorire l'applicazione del "Framework Nazionale per la Cybersecurity e la Data Protection" e dei "Controlli essenziali di cybersecurity", opportunamente aggiornati in linea con il quadro della minaccia, da parte della PA, delle imprese e delle PMI.