SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**

M6 - Certification and Frameworks for Organizations and management systems

Contents

Data center certification

HIGH FUNCTIONAL CAPABILITIES

Data centers and facilities play an important role in protecting information security, its *continuity* and, in particular, **availability** of information.

In some cases, in order to be **competitive**, organizations need to signal to **investors**, **customers** and the **market** that their data center and facilities have high functional capabilities, as demonstrated in the design documents, but also verify that the system design itself is consistent with **uptime goals**. Certification helps align infrastructure design with corporate mission, ensuring that the organization's significant capital investment produces the desired result.

TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION

What is Tier Certification?

Developed by Uptime Institute, the Tier Certification is a measure of data center infrastructure's capability to meet the **performance level** the business depends on.

A data center's **tier** certification can be based on Tier Standards, which are based on an unbiased set of infrastructure and operating criteria.

[Source: uptimeinstitute.com]

TIER Certification for data centers

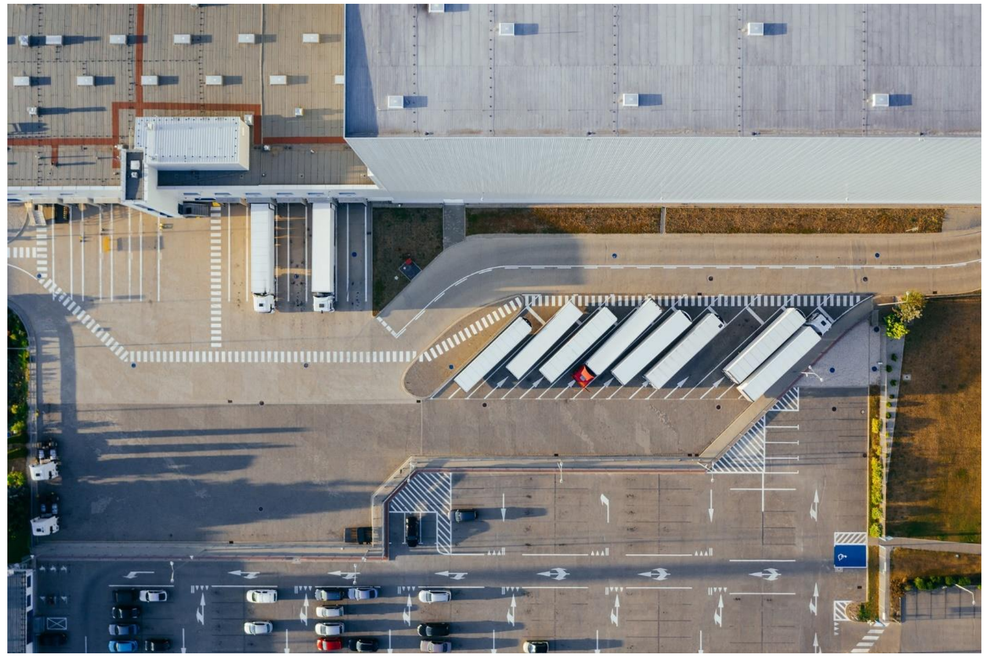
UPTIME INSTITUTE TIER CERTIFICATION

What are the key features of Tier Standard?

Tier Standards are performance-based, not prescriptive. Any design solution that meets the requirements for availability, redundancy, and fault tolerance is *acceptable*. This latitude allows you to incorporate a wide variety of infrastructure and system solutions to best meet the organization's goals for IT **operations**, **costs**, **sustainability**, and **uptime**.

Technology neutral: in an ever-changing technology landscape, Tier classification does not require or rely on any fixed set of technologies. The Standards are able to encompass specific solutions for data center systems and engineering, such as modular configurations, OCP, and leading-edge power and cooling approaches.
Tier Standard criteria is vendor-neutral and unbiased (it does not relate to specific brands).

[Source: uptimeinstitute.com]



TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION

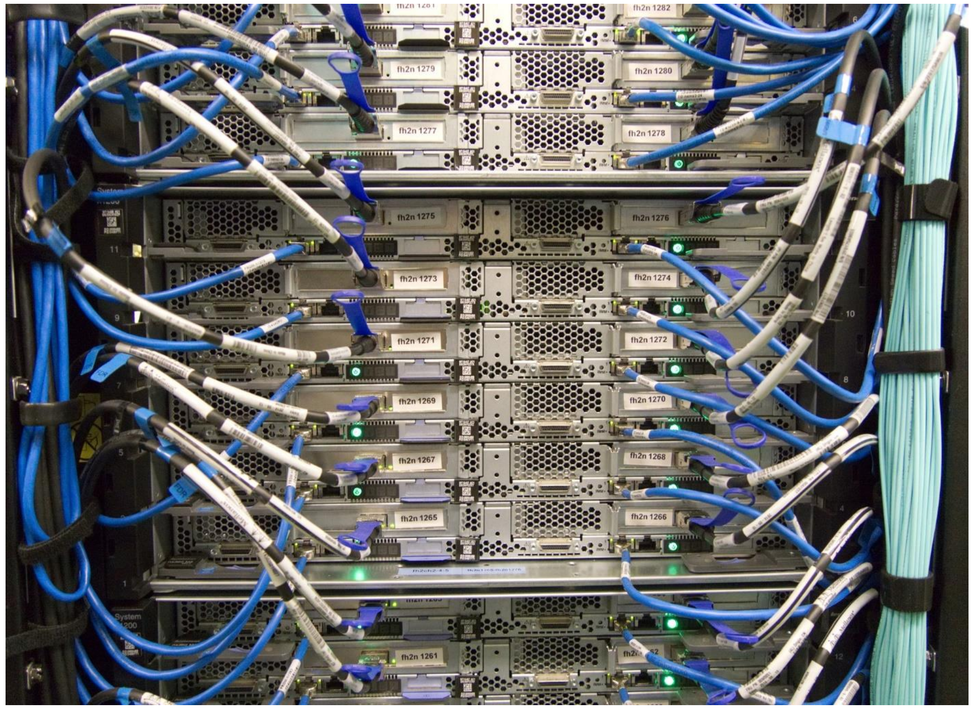
What are the key features of Tier Standard?

Flexible: The performance-based nature of the Tier standards gives organizations flexibility to comply with local statutes, codes, and regulations.

Lifecycle: Beginning with the Tier Standard in the Design Document phase and continuing with the Constructed Facility and Operational Sustainability phases, the Tier Standard has the organization covered.

Certification: The Standard is administered by the author of the standard itself.

[Source: uptimeinstitute.com]



TIER Certification for data centers

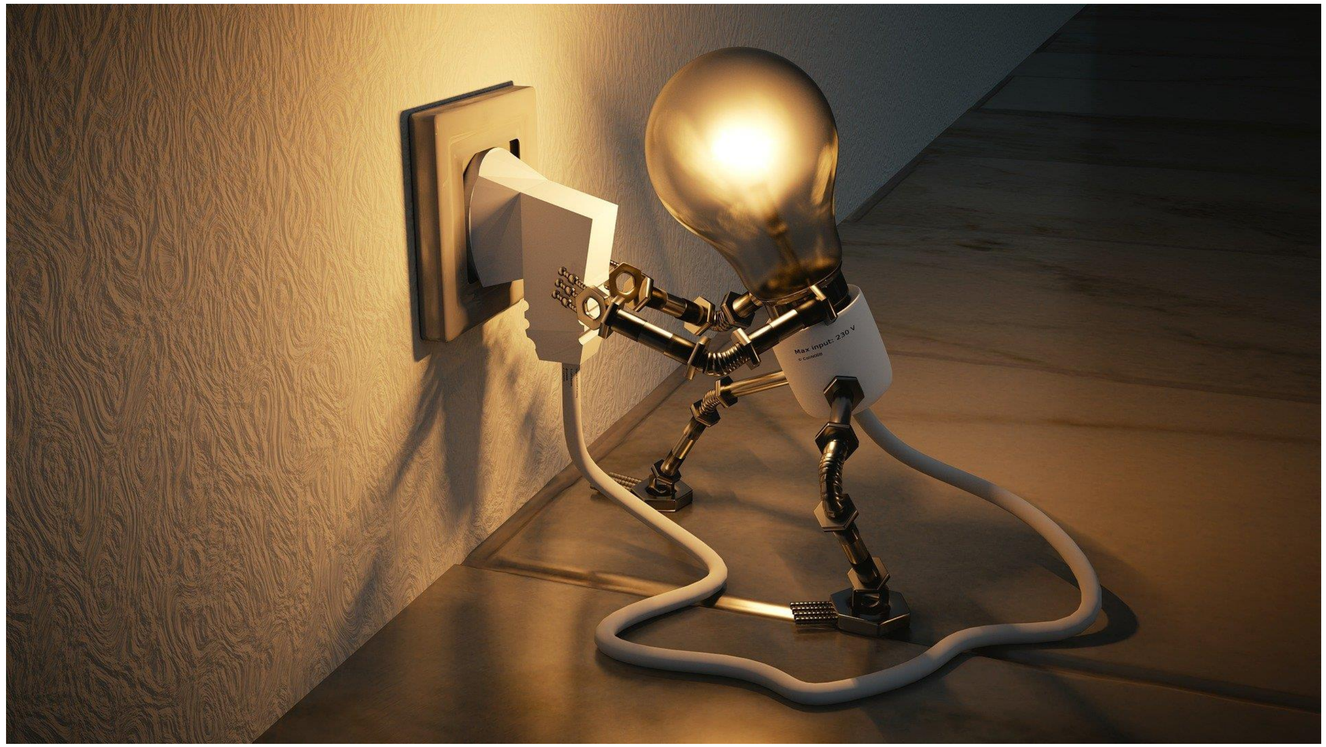
UPTIME INSTITUTE TIER CERTIFICATION

Data Center Tier Certification
Uptime Institute data center classifications are divided into four Tiers that match a particular business function and define criteria for **maintenance**, **power**, **cooling** and **fault** capabilities.

The Tiers are progressive, so each Tier incorporates the requirements of the lower Tiers. This progression does not mean that a Tier IV data center is better than a Tier II — it means that these levels fit **differing business operations**.

The definitions and benefits of the Tiers are set in our topology standard and focus on the data center infrastructure.

[Source: uptimeinstitute.com]



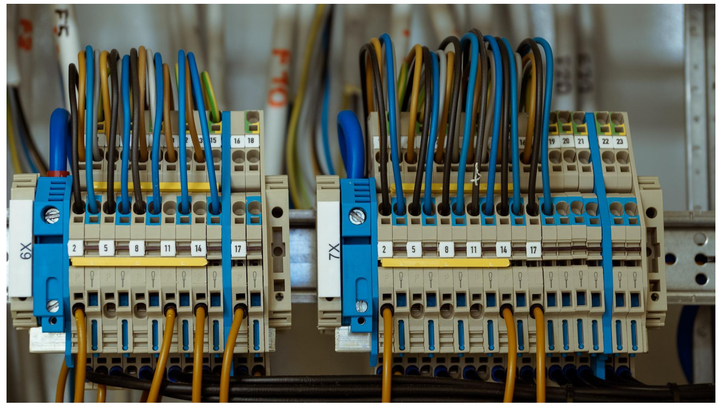
TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION

Data Center Tier Certification

Operational sustainability is the second essential component of data Tier classification. It refers to the **behaviors** and **risks** apart from infrastructure design that determine the ability of the data center to *meet long-term business goals*. Data center owners can align their management style to a Tier to achieve these goals, as management behavior is essential to operational sustainability.

[Source: uptimeinstitute.com]



Together, **topology** and **operational sustainability** establish the *performance criteria* for data centers to follow. Data center owners may also want to consider other factors, such as building codes, regional weather, security and property usage. Uptime institute topology and operational sustainability standards do not cover these factors because they vary in every case. It is ultimately up to the owner to determine which Tier is best for their business needs.

TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION

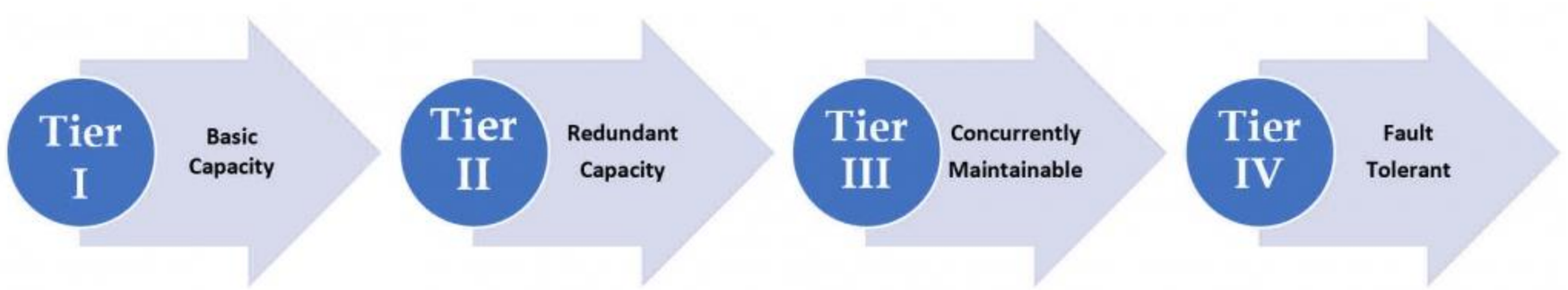
What a Tier Classification Means for a Data Center and Its Infrastructure

The data center Tier definitions define **criteria**, but not **specific technology** options or design choices to meet the Tier. Tiers are flexible enough to allow for many solutions that meet performance goals and compliance regulations. Many solutions lead to engineering innovation and uniqueness across data centers. Each data center can decide the best way to meet the Tier criteria and business goals.

[Source: uptimeinstitute.com]

TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION - TIER LEVELS



[Source: uptimeinstitute.com]

TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION - TIER LEVELS

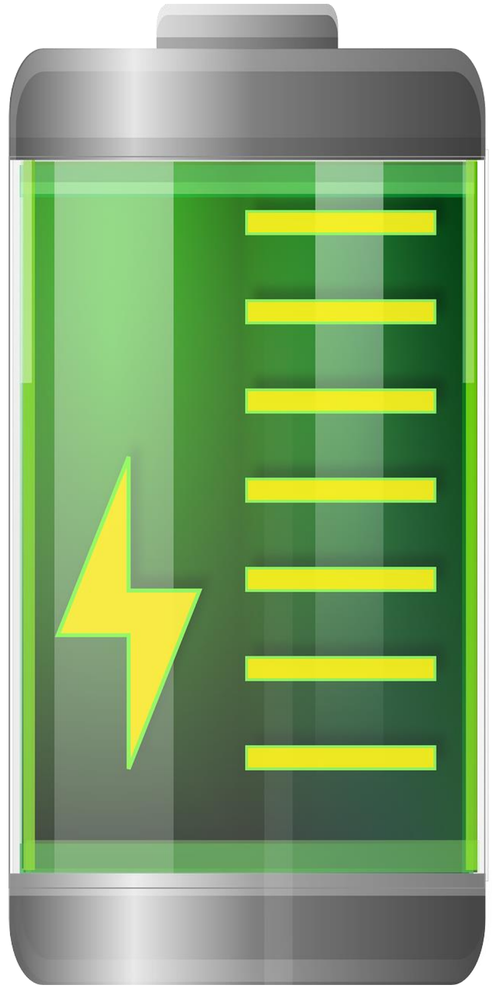
Tier I

A Tier I data center is the **basic capacity level** with infrastructure to support information technology for an office setting and beyond. The requirements for a Tier I facility include:

- An uninterruptible power supply (UPS) for power sags, outages, and spikes.
- An area for IT systems.
- Dedicated cooling equipment that runs outside office hours.
- An engine generator for power outages.

Tier I protects against disruptions from human error, but not unexpected failure or outage. Redundant equipment includes *chillers, pumps, UPS modules, and engine generators*. The facility will have to *shut down completely* for preventive maintenance and repairs, and failure to do so increases the risk of unplanned disruptions and severe consequences from system failure.

[Source: uptimeinstitute.com]



TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION - TIER LEVELS

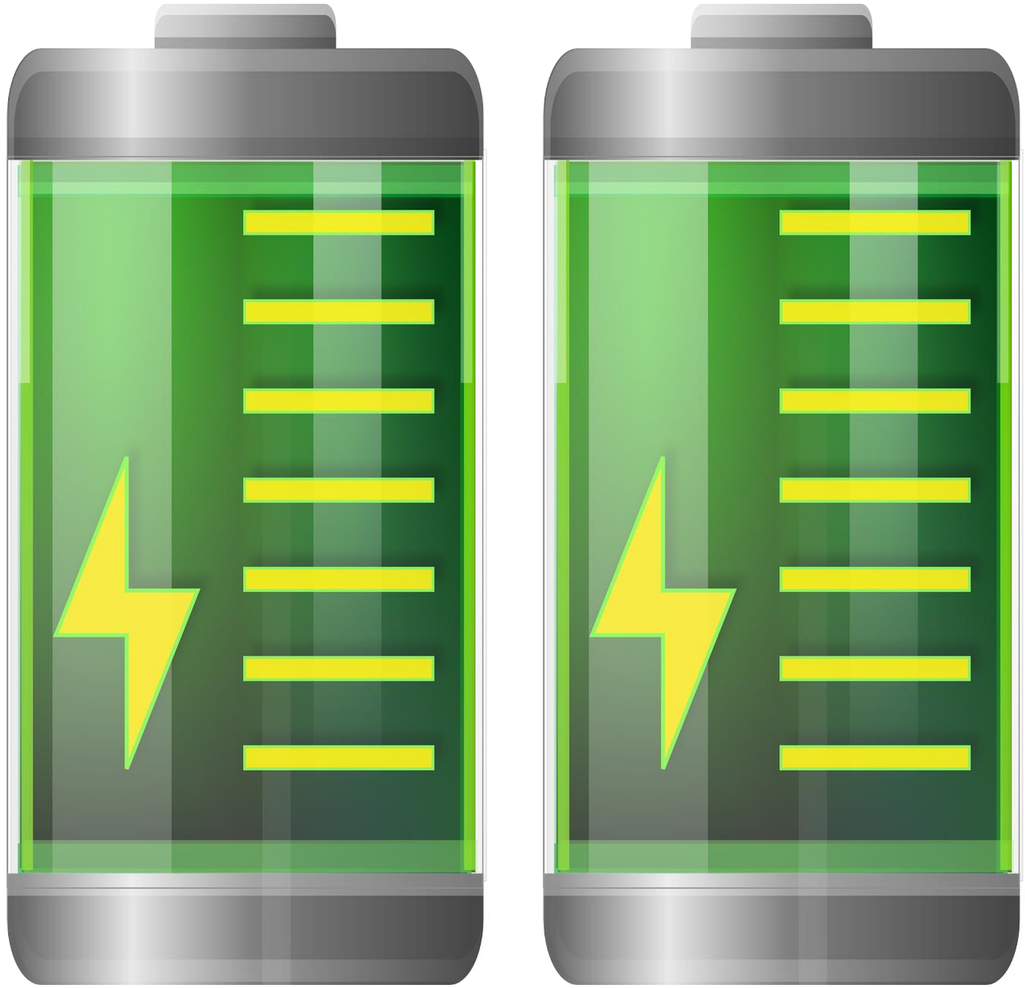
Tier II

Tier II facilities cover **redundant** capacity components for power and cooling that provide better maintenance opportunities and safety against disruptions. These components include:

- Engine generators.
- Energy storage.
- Chillers.
- Cooling units.
- UPS modules.
- Pumps.
- Heat rejection equipment.
- Fuel tanks.
- Fuel cells.

The distribution path of Tier II serves a **critical environment**, and the components can be removed *without shutting it down*. Like a Tier I facility, unexpected shutdown of a Tier II data center *will affect the system*.

[Source: uptimeinstitute.com]



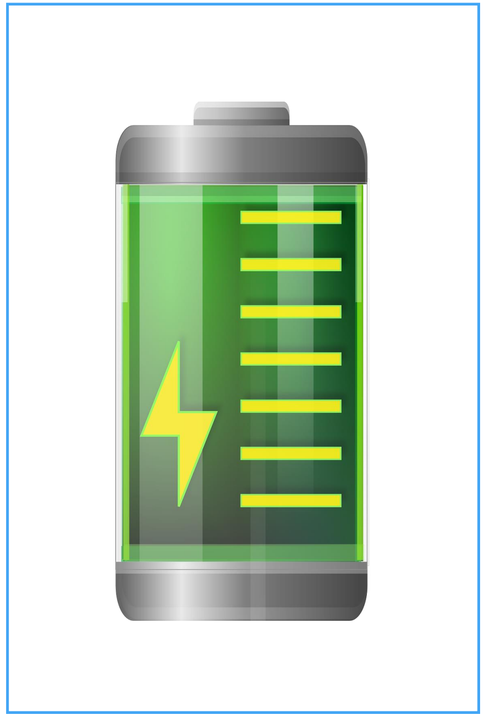
TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION - **TIER LEVELS**

Tier III

A Tier III data center is **concurrently maintainable** with redundant components as a key differentiator, with redundant distribution paths to *serve the critical environment*. Unlike Tier I and Tier II, these facilities require no shutdowns when equipment needs maintenance or replacement. The components of Tier III are *added* to Tier II components so that *any part can be shut down without impacting IT operation*.

[Source: uptimeinstitute.com]



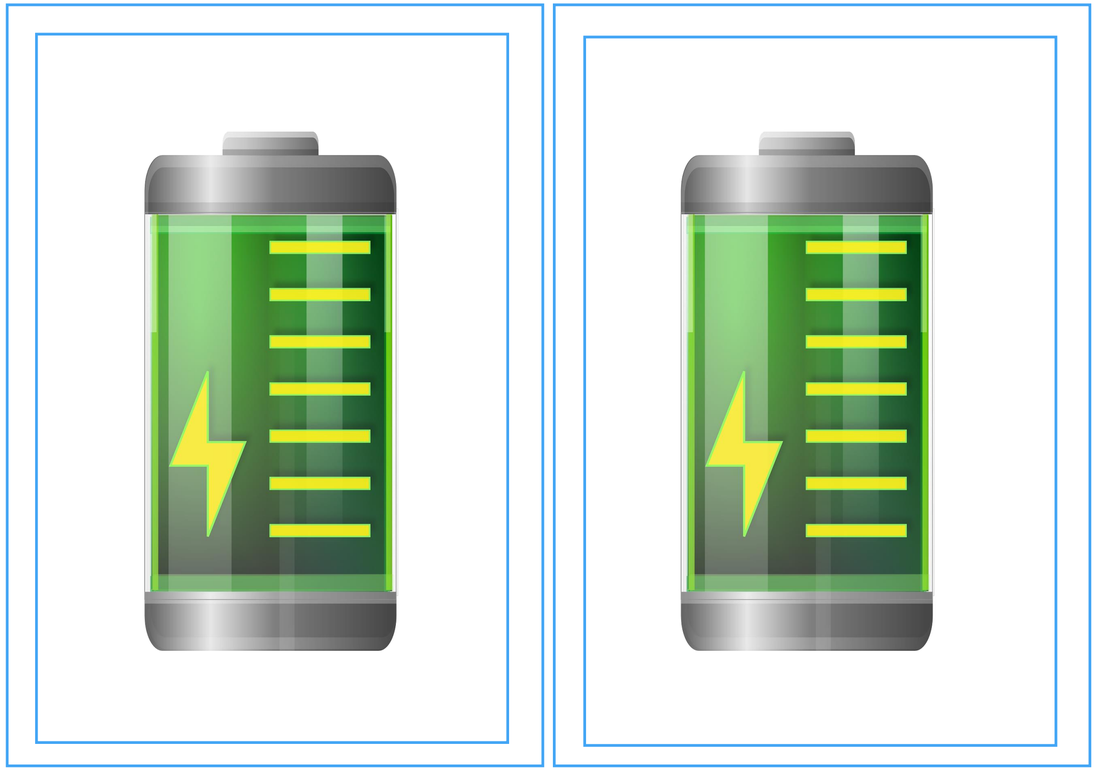
TIER Certification for data centers

UPTIME INSTITUTE TIER CERTIFICATION - TIER LEVELS

Tier IV

A Tier IV data center has **several independent** and **physically isolated** systems that act as redundant capacity components and distribution paths. The **separation** is necessary to prevent an event from compromising both systems. *The environment will not be affected by a disruption from planned and unplanned events*. However, if the redundant components or distribution paths are shut down for maintenance, the environment may experience a higher risk of disruption if a failure occurs.

Tier IV facilities add **fault tolerance** to the Tier III topology. When a piece of equipment fails, or there is an interruption in the distribution path, *IT operations will not be affected*. All of the IT equipment must have a fault-tolerant power design to be compatible. Tier IV data centers also require continuous cooling to make the environment **stable**.



[Source: uptimeinstitute.com]

More specific resources are available at **uptimeinstitute.com/resources**

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

Nist framework publication is the result of an ongoing collaborative effort involving **industry**, **academia**, and **U.S. government**.
The National Institute of Standards and Technology (NIST) launched the project by convening private- and public-sector organizations and individuals in 2013. Published in 2014 and revised during 2017 and 2018, this Framework for Improving Critical Infrastructure Cybersecurity has relied upon eight public workshops, multiple Requests for Comment or Information, and *thousands of direct interactions with **stakeholders** from across all sectors of the United States along with many sectors from around the world*.

[source: NIST Framework publication, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

The Framework focuses on using **business drivers** to guide cybersecurity activities and *considering cybersecurity risks as part of the organization's risk management processes*.

The Framework consists of three parts:
- the Framework **Core**,
- the Implementation **Tiers**,
- and the Framework **Profiles**.

[source: NIST Framework publication, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

The Framework **Core** is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Core provide detailed guidance for developing individual organizational **Profiles**. Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources.
The **Tiers** provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives.

[source: NIST Framework publication, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

While this document was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in **any sector** or **community**. The Framework enables organizations – *regardless of size, degree of cybersecurity risk, or cybersecurity sophistication* – to apply the principles and best practices of risk management to improving security and resilience.
The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today.

[source: NIST Framework publication, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

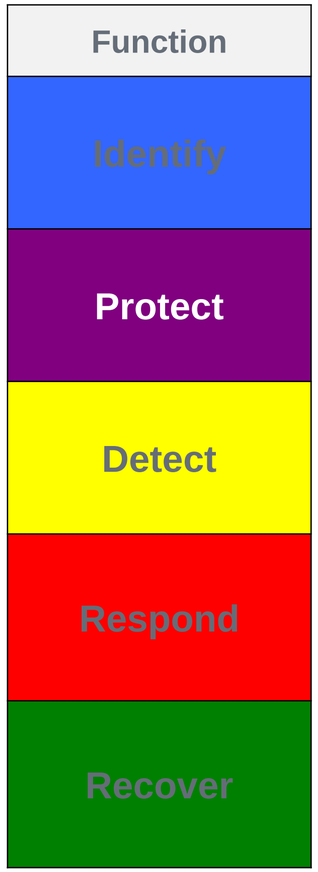
- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

[source: NIST Framework presentation, v.1.1]

Fuctions within the NIST Framework

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY



- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

[source: NIST Framework presentation, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions | 23 Categories | 108 Subcategories | 6 Informative References

[source: NIST Framework presentation, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

Implementation tiers →

	1	2	3	4
	Partial	Risk Informed	Repeatable	Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk**[1.1] • benefits my sharing or receiving information from outside parties			

[source: NIST Framework presentation, v.1.1]

NIST FRAMEWORK

FOR IMPROVING
CRITICAL INFRASTRUCTURE CYBERSECURITY

- Applicability for **all** system lifecycle phases
- Enhanced guidance for managing cybersecurity within **supply chains** and for **buying decisions**
- New guidance for **self-assessment**
- Better accounts for **Authorization**, **Authentication**, **and Identity Proofing**
- Incorporates emerging **vulnerability information** (a.k.a., Coordinated Vulnerability Disclosure)
- Administratively updates the **Informative References**

[source: NIST Framework presentation, v.1.1]

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION

Cini has improved the Framework Core by introducing

- new categories and subcategories dedicated to **data protection** topics (Section 4.1);

- **Contextualization Prototypes**, a new tool that support and facilitates the denition of contextualizations (Section 4.2)

[source: CINI Framework presentation, AFP 2020]

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION

GOALS of the CINI Italian National Framework for cybersecurity and data protection

Design a **cybersecurity framework**

- that uses a **risk-based approach**
- easily **adaptable** to the heterogeneous characteristics of the **Italian context**
- **coherent** with national/international regulations
- aligned to existing **standards**
- that takes into account **data protection**

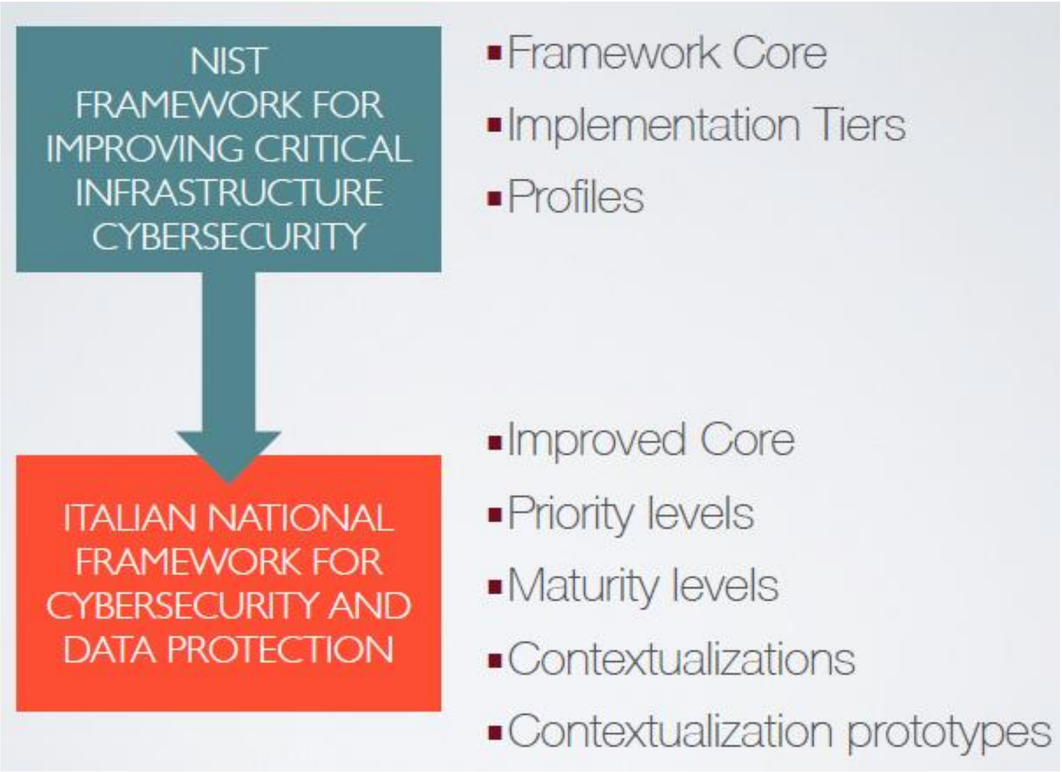
[source: CINI Framework presentation, AFP 2020]

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION

Lead to the Italian national framework for cybersecurity and data protection.

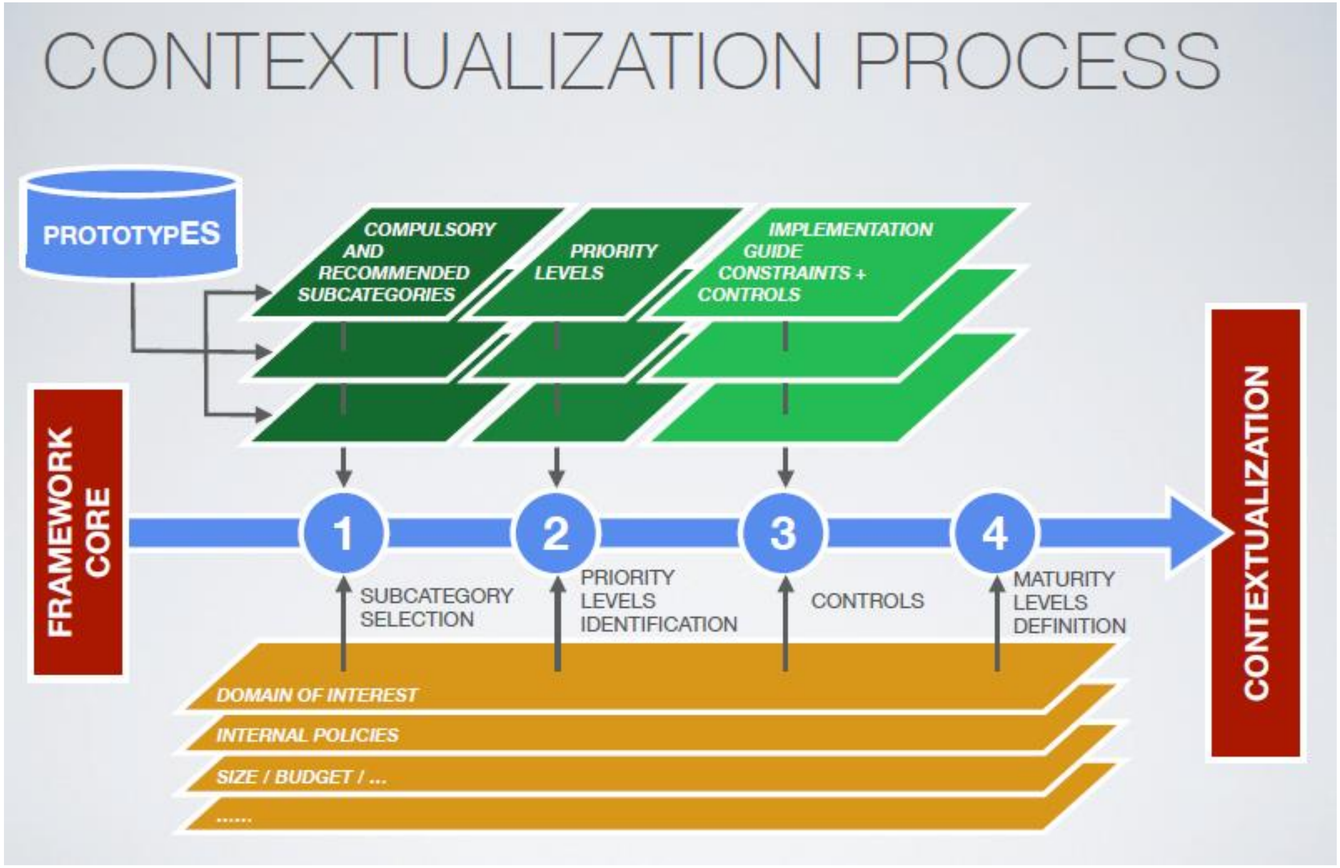
It inherits the core structure and contents from NIST CSF 1.1 and has a hierarchically organized collection of 117 enabling activities.



[source: CINI Framework presentation, AFP 2020]

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION



[source: CINI Framework presentation, AFP 2020]

CONTEXTUALIZATION

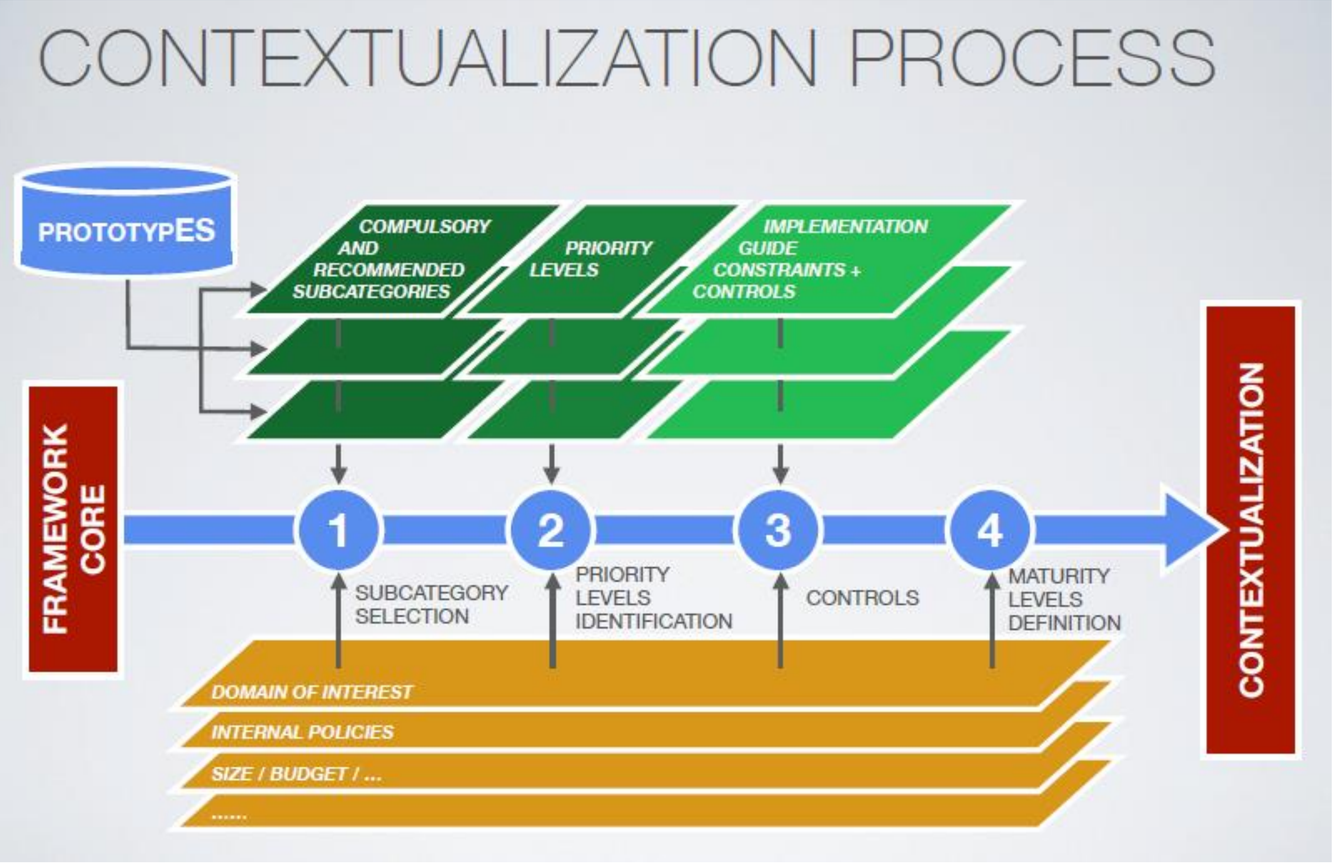
Applying the framework to a given organization requires an appropriate **contextualization**:

- Selection of core subcategories applicable to the target domain of interest
- Identification of implementation priority levels for all the selected subcategories
- Definition of appropriate controls for subcategory implementation, possibly associated to maturity levels

Parts of a contextualization may be applicable to several realities that *share* some requirements (e.g. compliance to common regulations, adoption of the same best practices, etc.)

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION



[source: CINI Framework presentation, AFP 2020]

CONTEXTUALIZATION PROTOTYPES

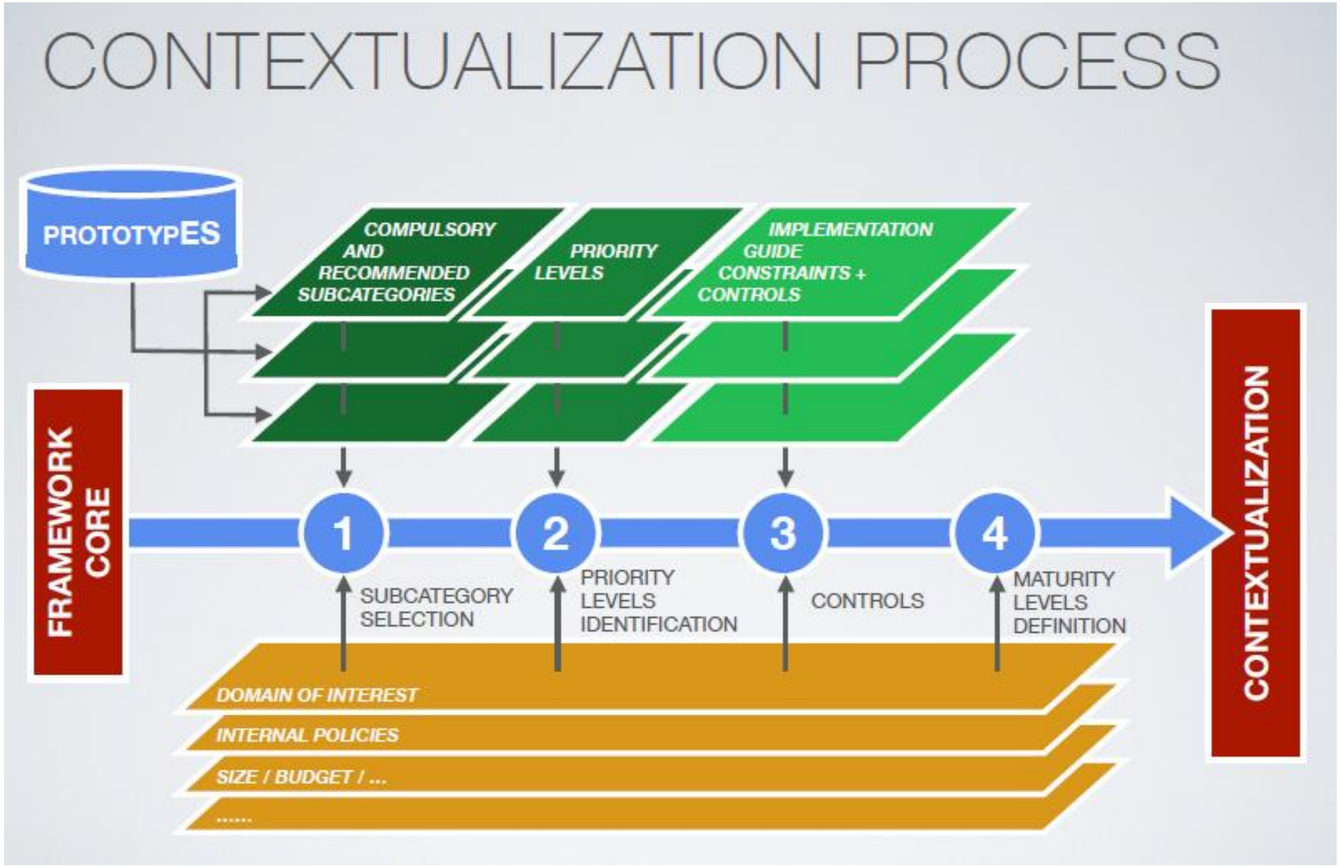
Contextualization prototypes allow the definition of "*templates*" that can be used to embed specific requirements during the contextualization process.

Prototypes can be used, for example, to capture through the Framework requirements defined by:

- **regulations** that impose specific requirements linked to cybersecurity or data protection aspects;
- **technical documents** that include specific controls for cybersecurity or data protection processes;
- **best practices**.

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION



[source: CINI Framework presentation, AFP 2020]

CONTEXTUALIZATION PROTOTYPES

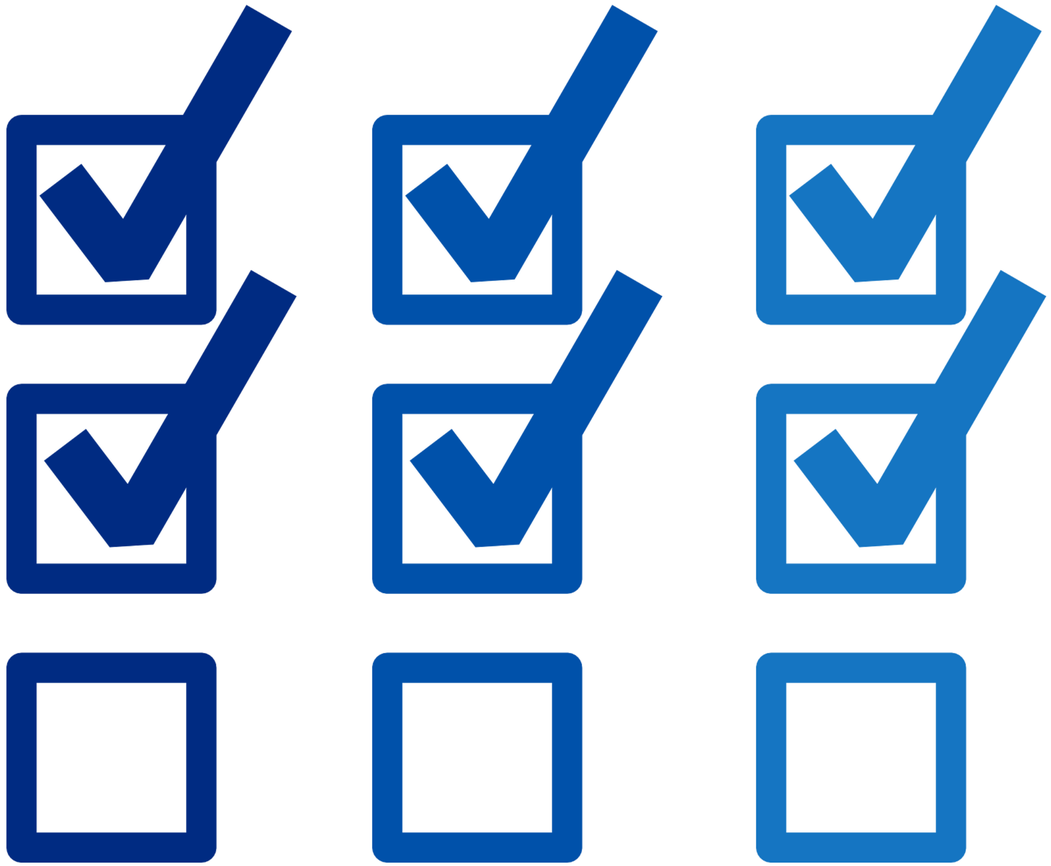
▪for each core subcategory defines an **implementation class**:
- *mandatory / recommended / free*

▪for each core subcategory it may define a suggested **priority** level

▪it includes an implementation guide, a document that describes:
- the **domain of interest** for the prototype
- further **constraints** on subcategory selection (if any)
- A list of optional **controls** for the considered subcategories

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION



CONTEXTUALIZATION PROTOTYPES

▪for each core subcategory defines an **implementation class**:
- *mandatory* / *recommended* / *free*

▪for each core subcategory it may define a suggested priority level

▪it includes an implementation guide, a document that describes:
- the **domain of interest** for the prototype
- further **constraints** on subcategory selection (if any)
- A list of optional **controls** for the considered subcategories

[source: CINI Framework presentation, AFP 2020]

CINI – Consorzio interuniversitario nazionale per l'informatica

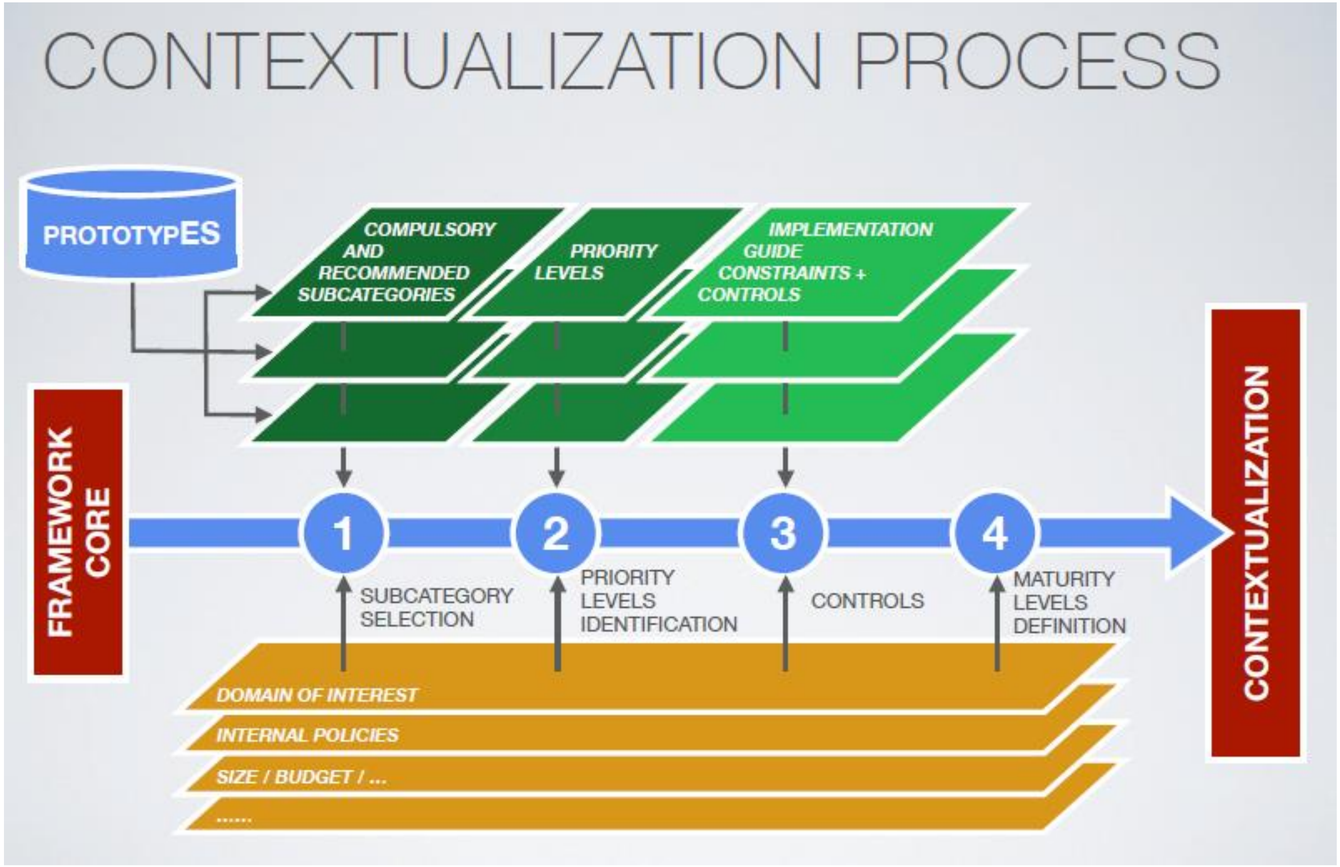
ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION

Subcategory	Class	Priority	Informative References
DP-ID.AM-7: Roles and responsibilities inherent to data protection and processing activities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	mandatory	HIGH	GDPR - Artt. 24, 26-29, 37-39
DP-ID.AM-8: Data processing activities are identified and inventoried	mandatory	HIGH	GDPR - Art. 30
DP-ID.DM-4: Processes for exercising data subject rights (access, rectification, erasure, etc.) are established , implemented and documented	mandatory	HIGH	GDPR - Art 15-22
DP-RS.CO-6: Incidents that cause personal data breaches are investigated, documented and reported to the appropriate authorities and to the data subjects	mandatory	HIGH	GDPR - Artt. 33, 34

[source: CINI Framework presentation, AFP 2020]

CINI – Consorzio interuniversitario nazionale per l'informatica

ITALIAN NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION



[source: CINI Framework presentation, AFP 2020]

The Framework is experiencing a growing adoption among Italian organizations of various sizes

- large organizations already use the NIST CSF => straightforward mapping

- Italian **NIS authorities** published their guidelines for OESs using the Framework as a common baseline Next steps:

- Improve **internationalization** (currently the core is only available in EN)

- Alignment with **other frameworks** (NIST Privacy Framework, ISO 27701/29100)

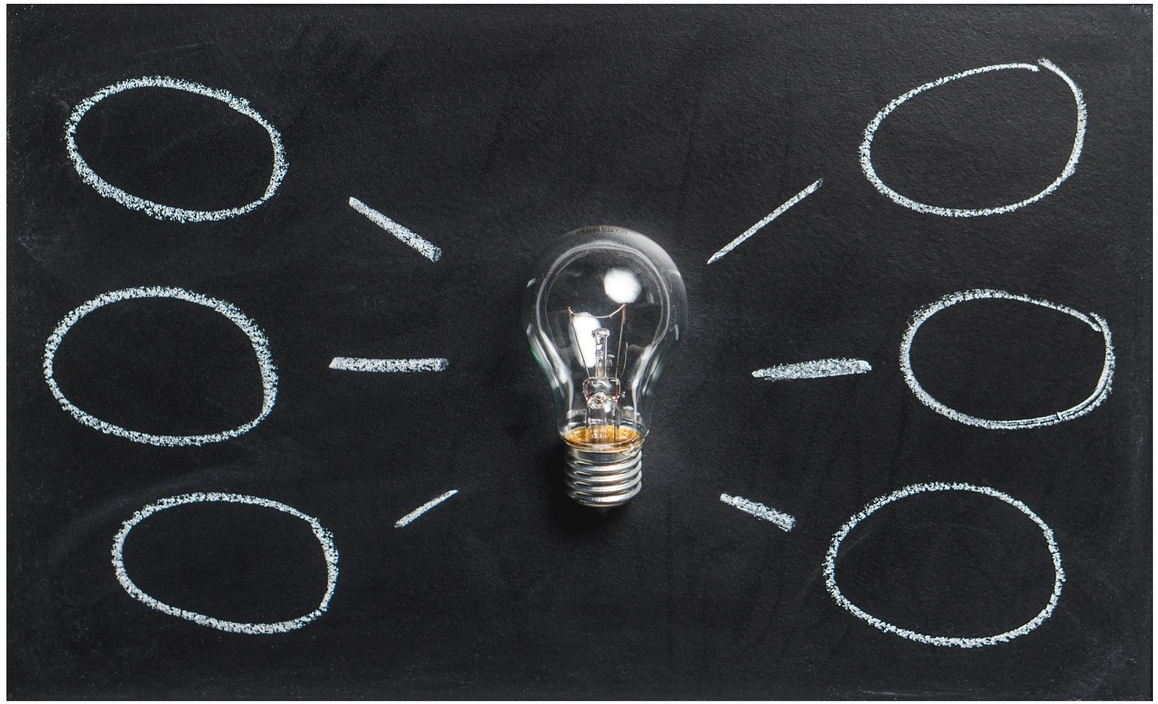
- Implementation of a **quantitative** security assessment methodology on top of the Framework

EU strategies for cybersecurity

2013 TO PRESENT

- EU Cybersecurity Strategy (2013)
- European Agenda on Security (2015)
- Digital Single Market Strategy (2015)
- Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016)

[Source: EU cybersecurity initiatives, EU Commission, 2017]



NIS Directive

«NETWORK AND INFORMATION SECURITY»

Directive on Network and Information Security

In 2013 the Commission proposed the Directive on security of network and information systems (NIS Directive) aiming at ensuring a high common level of cybersecurity in the EU.

After an approval process, the Directive entered into force in August 2016.

[Source: EU cybersecurity initiatives, EU Commission, 2017]

NIS Directive

«NETWORK AND INFORMATION SECURITY»

The Directive builds on **three** main *pillars*:

1) ensuring Member States **preparedness** by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (**CSIRT**) and a competent **national NIS authority**;

[Source: EU cybersecurity initiatives, EU Commission, 2017]

NIS Directive

«NETWORK AND INFORMATION SECURITY»

2) ensuring **cooperation among all the Member States**, by setting up a '*Cooperation Group*', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a '*CSIRT* Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;

[Source: EU cybersecurity initiatives, EU Commission, 2017]

NIS Directive

«NETWORK AND INFORMATION SECURITY»

3) ensuring a **culture of security** across sectors which are vital for our economy and society and moreover rely heavily on information and communications technologies (ICT). Businesses with an important role for society and economy that are identified by the Member States as operators of essential services under the NIS Directive will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include **energy**, **transport**, **water**, **banking**, **financial market infrastructures**, **healthcare** and **digital infrastructure**. Also key digital service providers (**search engines**, **cloud computing** services and **online marketplaces**) will have to comply with the security and notification requirements under the new Directive. Similar requirements already apply to telecom operators and internet service providers through the EU telecoms regulatory framework.

[Source: EU cybersecurity initiatives, EU Commission, 2017]

NIS Directive

ITALIAN ROADMAP

Cyber security is one of the interventions envisaged by the **National Recovery and Resilence Plan** (PNRR) transmitted by the Government to the European Commission on 30 April 2021.

At European Union level, Directive (EU) 2016/1148 of 6 July 2016 sets out measures for a high common level of security of networks and information systems in the Union (so-called NIS – Network and Information Security ") in order to achieve a "*high level of security of the network and information systems at national level, helping to increase the common level of security in the European Union*".

The directive was **transposed** into Italian law with legislative decree no. 65 of 18 May 2018, which therefore dictates the legislative framework of the measures to be adopted for the security of networks and data information systems and identifies the competent subjects to implement the obligations established by the NIS directive.

New challanges for ICT and cybersecurity law

The most recent reports on information policy sent to Parliament (such as the Annual Report to Parliament and the National Security Document) highlight the significant impact they have had - on the life of individuals, as well as on the political-economic balance and on the same way of "playing the democratic game" - the rapid, massive diffusion of **new technologies** and the consequent**, instant accessibility** on a global level of **news** and **data**, and therefore of knowledge, but also of mystified or tout court unfounded representations and distorted or falsified narratives.

New challanges for ICT and cybersecurity law

The current **health** and **geopolitical** situation have confirmed the importance of protecting IT and information systems, making data and IT protection a key element for the security of any organization regardless of the reference sector. Consequently, never like today the existing laws and regulations on network and system security become a **point of reference** for all companies that intend to increase their level of security and awareness regarding cyber threats and risks.

In 2020, the European Commission **revised the NIS** (Network and Information Technology) Directive, questioning the efficiency of the measures adopted. In the same year, the National Cyber Security Perimeter was first implemented, a plan for the protection of national computer networks and systems.

New challanges for ICT and cybersecurity law

The new Commission proposal aims to address the deficiencies of the previous NIS Directive, to adapt it to the current needs and make it future-proof.

To this end, the Commission proposal expands the scope of the current NIS Directive by **adding new sectors** based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, *it leaves some flexibility for Member States to identify smaller entities with a high security risk profile*.

The proposal also eliminates the distinction between *operators of essential services* and *digital service providers*. Entities would be classified based on their importance, and divided respectively in **essential** and **important** categories with the consequence of being subjected to *different supervisory regimes*.

[Source: digital-strategy.ec.europa.eu]

New challanges for ICT and cybersecurity law

The proposal strengthens security requirements for the companies, by imposing a **risk management approach** providing a *minimum list* of *basic security elements* that have to be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

Furthermore, the Commission proposes to address security of **supply chains** and **supplier relationships** by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships.

At the European level, the proposal strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the **Commission** and **ENISA**, will carry out coordinated risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

[Source: digital-strategy.ec.europa.eu]

New challanges for ICT and cybersecurity law

The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

The proposal also enhances the role of the **Cooperation Group** in *shaping strategic policy* decisions on emerging technologies and new trends, and increases information sharing and cooperation between Member State authorities. It also enhances **operational cooperation** including on cyber crisis management.

The Commission proposal establishes a **basic framework** with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creating an EU registry on that operated by the European Union Agency for Cybersecurity (ENISA).

[Source: digital-strategy.ec.europa.eu]

Some online resources

Enisa website

- www.enisa.europa.eu

Nist cyberframework:

- https://www.nist.gov/cyberframework

Cybersecurity national lab:

- https://cybersecnatlab.it/

Nis Directive full text Directive (EU) 2016/1148:

- https://www.enisa.europa.eu/topics/nis-directive#:~:text=Directive%20(EU)%202016/1148.

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Antonio **Belli**
Simone **Soderi**
antonio.belli@unipd.it
simone.soderi@unipd.it

Thanks for your attention!

M1 - Certification and Frameworks for Organizations and management systems