CAEED - Security of IT Systems, main frameworks available with a special focus on some security issues related to the smart metering

OVERVIEW

1 – Regulatory framework

2 – IT security in the IT environment

3 – Cybersecurity assessment and NIST framework

4 – 2G Smart Metering

5 – Cybersecurity in the in the Smart metering: the Italian experience

6 – Conclusions

Regulatory framework – EU digitalization

Energy digitalization in the European Regulatory Framework

Energy Efficiency Directive – (EU) 2018/2002. → enabling the digitalization from demand side management.

Electricity Directive - (EU) 2019/944 and the Regulation on the **internal market for electricity – (EU) 2019/943** → addressing data exchange including the deployment of smart meters in the electricity sector.

The Communication on "**An EU strategy for Energy System Integration**" - adopted in July 2020 → set out key actions to drive the energy transition, including a "system-wide Digitalisation of Energy Action Plan that could accelerate the implementation of digital solutions and energy system integration across multiple energy carriers, infrastructures and consumption sectors".

General Data Protection Regulation (EU) 2016/679 → that created a transparent and well- functioning data protection framework.

Commission published a **European Strategy on AI in April 2018** → in order to place people at the centre of the **AI development**. In 2021, the EU Commission presented a regulatory proposal on artificial intelligence (**Artificial Intelligence Act**) which aims to provide AI developers, deployers and users with clear requirements and obligations regarding specific uses of AI.

With regards to **Blockchains** → the European Union wants to be a leader in blockchain technology, becoming an innovator in blockchain and a base to innovative platforms, applications and companies. European Parliament Resolution of 3 October 2018 on Distributed Ledger Technologies (**DLT**) and **Blockchains**: building trust with disintermediation (2017/2772(RSP)) underlined the related opportunities in the energy and environment-friendly applications.

.

Regulatory framework – EU cybersecurity strategy

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new **EU Cybersecurity Strategy** at the end of 2020.

- NIS Directive (introduced in 2016)
- NIS2 Directive (came into force in 2023):

The Strategy covers the **security of essential services** such as hospitals, **energy grids** and railways.

- Security Incident Response Team (CSIRT)
- competent national Network and Information Systems (NIS) authority

- Cooperation Group to support and facilitate strategic cooperation

The Strategy focuses on **building collective capabilities** to respond to major cyberattacks and working with partners around the world to ensure international security and stability in cyberspace.

- Security culture across sectors that rely heavily on ICTs, such as energy

ENISA (European Union Agency for Cybersecurity) is the EU agency that deals with **cybersecurity**. It provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive.

- The Cybersecurity Act strengthens the role of ENISA. The agency now has a permanent mandate, and is empowered to contribute to stepping up both operational cooperation and crisis management across the EU.

- The Recovery Plan for Europe includes additional investments in cybersecurity

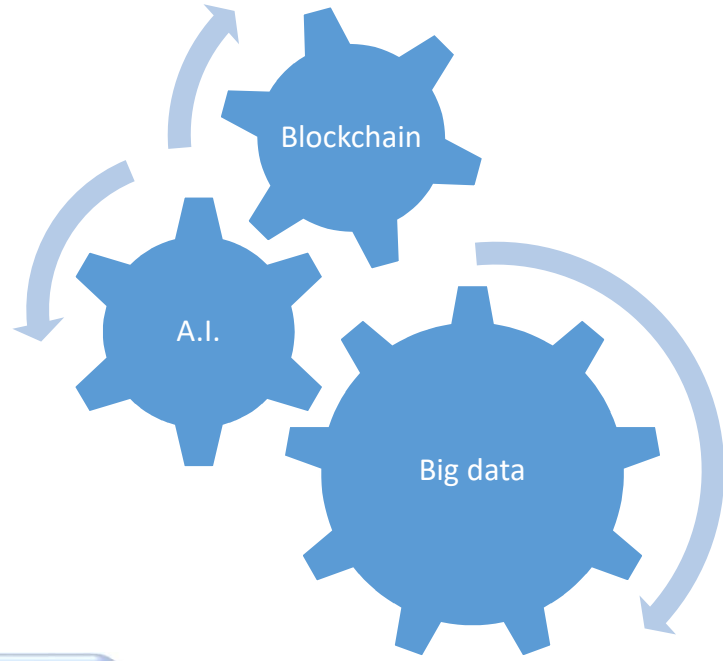
Regulatory framework – digitalization and cybersecurity

The energy digitalization challenges

Digitalization can improve processes efficiency (energy systems smarter, more connected, efficient and resilient, etc.**)**

Market design challenges

Digitalization raises new security and privacy concerns
(data breach, personal data stealing, business interruptions, etc.)



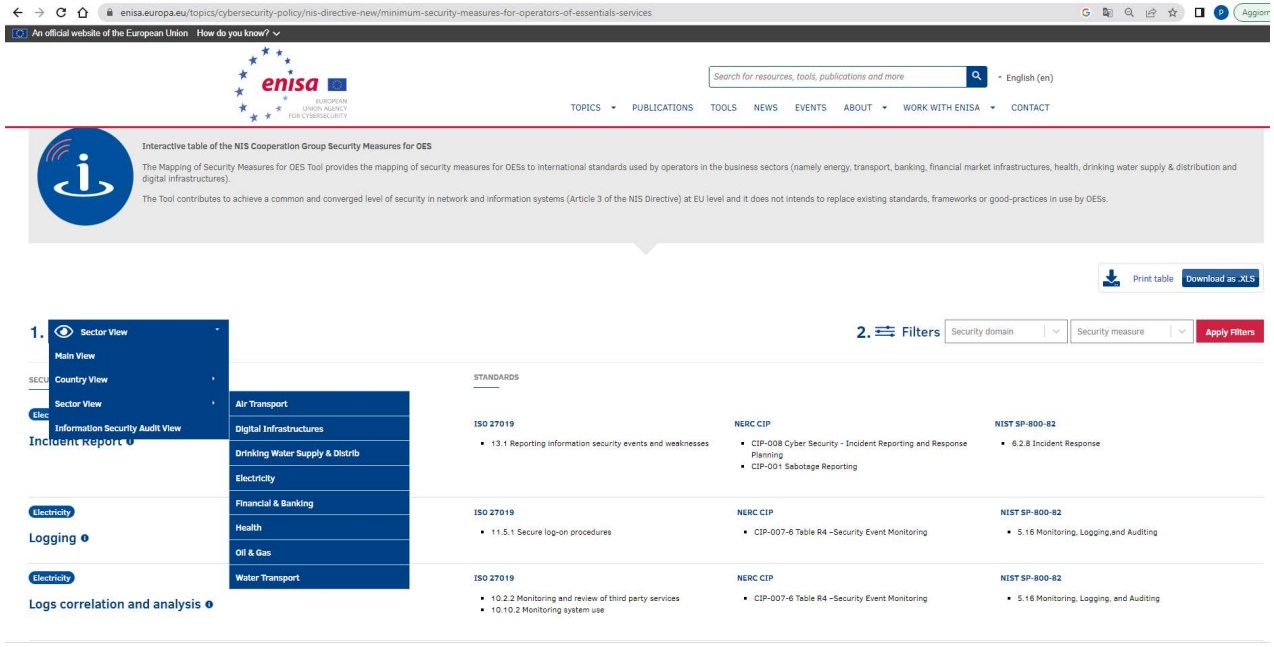
Regulatory framework – digitalization and cybersecurity

Minimum Security Measures for **O**perators of **E**ssentials **S**ervices

- **Interactive table of the NIS Cooperation Group Security Measures for OES**

✓ The Mapping of Security Measures for OES Tool provides the mapping of security measures for OESs to international standards used by operators in the business sectors (namely energy, transport, banking, financial market infrastructures, health, drinking water supply & distribution and digital infrastructures).

✓ The Tool contributes to achieve a common and converged level of security in network and information systems (Article 3 of the NIS Directive) at EU level and it does not intends to replace existing standards, frameworks or good-practices in use by OESs.



EXAMPLE

Incident Report
- 13.1 Reporting information security events and weaknesses (**ISO 27019**)
- CIP-008 Cyber Security - Incident Reporting and Response Planning (**NERC CIP**)
- CIP-001 Sabotage Reporting (**NERC CIP**)
- 6.2.8 Incident Response (**NIST SP-800-82**)

Logging
- 11.5.1 Secure log-on procedures ((**ISO 27019**))
- CIP-007-6 Table R4 –Security Event Monitoring (**NERC CIP**)
- 5.16 Monitoring, Logging, and Auditing (**NIST SP-800-82**)

Information system security incident response
- 13 Information security incident management (**ISO 27019**)
- CIP-008-5 Table R1 –Cyber Security Incident Response Plan Specifications (**NIST SP-800-82**)
- CIP-008-5 Table R2 –Cyber Security Incident Response Plan Implementation and Testing (**NIST SP-800-82**)
- 5.17 Incident Detection, Response, and System Recovery (**NIST SP-800-82**)

Human resource security
- 8. Human resource security (**ISO 27019**)
- CIP-004 Cyber Security - Personnel & Training (**NERC CIP**) ,
- CIP-004-6 Table R1 –Security Awareness Program (**NERC CIP**)
- CIP-004-6Table R3–Personnel Risk Assessment Program (**NERC CIP**)
- 6.2.1 Personnel Security (**NIST SP-800-82**)

Regulatory framework – AgID

- AgID has the task of coordinating public administrations in the implementation of the **Three-Year Plan** for information technology in Public Administration, ensuring consistency between the Italian and European digital agenda.
- AgID supports digital innovation and promotes the dissemination of digital skills, also in collaboration with international, national and local institutions and bodies.

- In Italy the Digital Transformation guidelines are written and updated by a technical agency of the Presidency of the Council of Ministers, called **AgID** (*Agency for Digital Italy*).
- The main purpose of the Agency is to guarantee the achievement of the Italian digital agenda objectives and contribute to the diffusion of information and communication technologies, with the aim of fostering innovation and economic growth.

Regulatory framework – AgID

IT security and risk management

both for facing the increasingly recurring cyber threats, and in terms of continuous monitoring to ensure the security of processes and data, with particular attention to personal data also in compliance with the European GDPR legislation

- **Governance**
  The information assets of the Public Administration is continuously exposed to cyber-type attacks, which are hostile activities towards an IT component, often carried out by exploiting the weaknesses of the human component (for example, inadequately trained personnel). Countering cyber threats has become an increasingly strong need as it guarantees not only the **availability, integrity and confidentiality of the information of the Public Administration information system**, but is the prerequisite for the **protection of the data**.

- **Monitoring**
  The **National Recovery and Resilience Plan (PNNR)**, the establishment of the **new National Cyber Security Agency** and the implementing decree of the national cyber security perimeter place **cyber security at the foundation of the digitization of the Public Administration**.

- **GDPR compliance**
  The protection of personal data is not only a regulatory necessity, but also an ethical choice that translates into guaranteeing and respecting the inviolable rights of people in compliance with the relationship of trust between the data subjects and the Institution.
  To ensure data protection, GSE adopts an approach in which **the security strategy and the consequent implementation derive**

IT Security in the IT environment

Information Technology General **Environment**

End **U**ser **C**omputing

IT Governance

Policies, standards, guidelines, procedure and technical instructions

Application security

Configuration (control and security settings), data exchange, program changes, program development

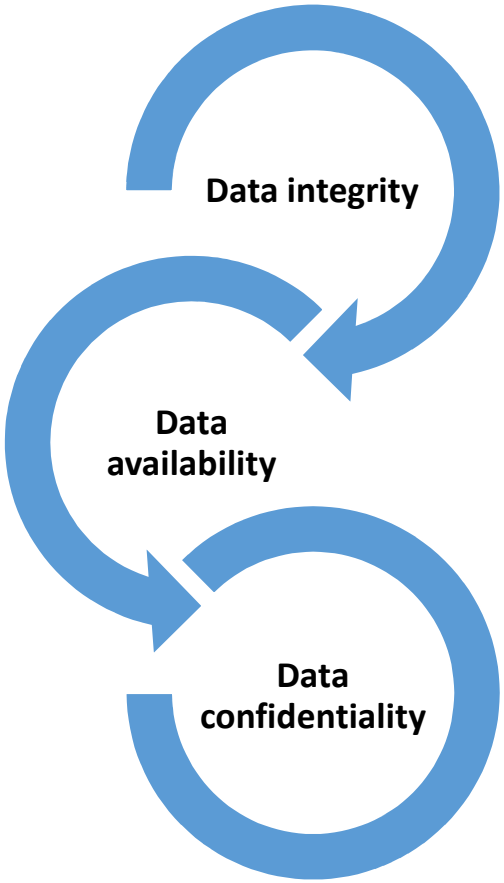
Database security

Configuration (control and security settings), data exchange and tables changes

Operating system, network and physical security

Configuration (control and security settings), vulnerability assessment, intrusion detection system, intrusion prevention system, physical and logical access controls.

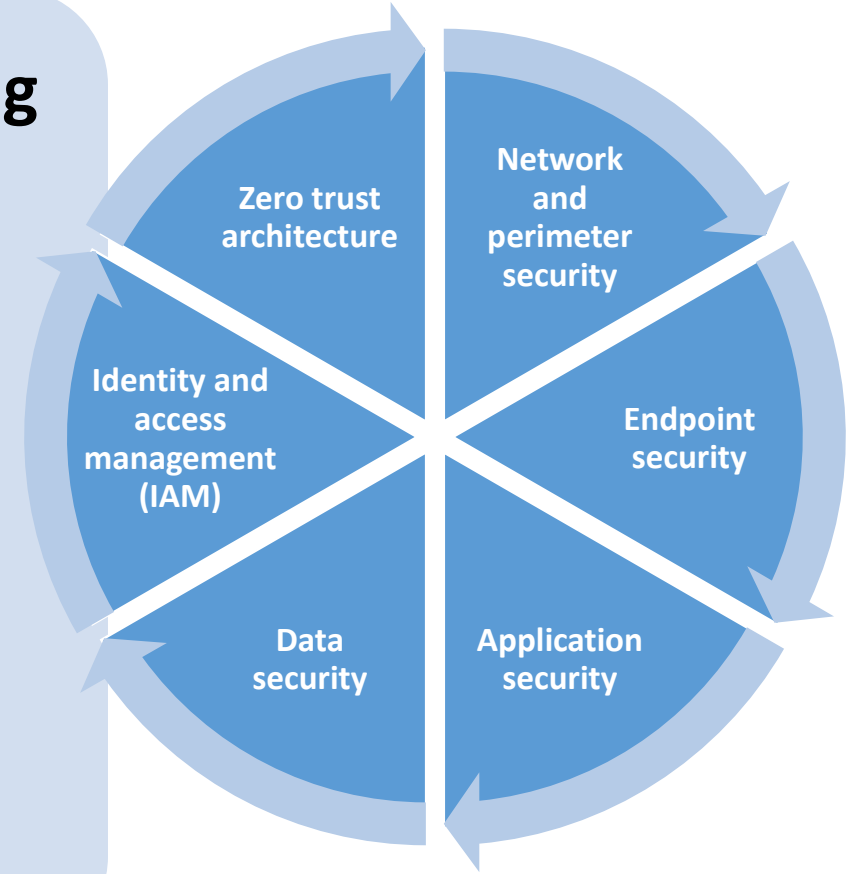
3 pillars of **Data Security** and **Cyber Security related IT Risks**



IT Security in the IT environment

How to identify the IT controls addressing cybersecurity organization risks?

- Clear understanding of the organization's business drivers and objectives
- Security considerations specific to its use of technology
- Company risk attitude and appetite (risk minimization)
- Privacy Risk management



IT Security in the IT environment - GDPR

Data Protection Office (DPO): GDPR in nutshell

The European Regulation on the Protection of Personal Data (**G**eneral **D**ata **P**rotection **R**egulation) has entered into force from May 24, 2016, and has been applied in Italy from May 25, 2018. Other provisions for the adaptation of the national legislation to the GDPR have been introduced by Legislative Decree no. 101 of August 10, 2018.

The **GDPR**, compared to previous discipline of 2003, emphasizes:

- the value, material too, of personal data in the light of technological innovation and globalization;
- the protection of interested parties and their rights towards the Data Controller, i.e. towards public Administrations and private Companies who process their data;
- the accountability of the Data Controller who must demonstrate that has put in place all the organizational and technical measures appropriate to their protection in the event of checks by the Supervisory Authorities or disputes.

***Personal Data* (art. 4.1, GDPR)**

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

***Processing of personal data relating to criminal convictions and offences (Judicial Data* - art. 10, GDPR)**

Personal data relating to criminal convictions and offences or related security measures.

***Processing of special categories of personal data (Special categories of personal data* - art. 9, GDPR)**

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

IT Security in the IT environment - GDPR

Privacy By Design e By Default

ART. 25: The GDPR provides for the obligation to ensure that the measures (also IT measures) adopted effectively implement the principles of privacy by design (data protection by design) and privacy by default (default setting that provides for the processing of only the data necessary for the declared purposes).

Contract management with the processors

ART. 28: The processor must protect the data according to the indications of the Data Controller with IT security measure and declare from the beginning of the processing operations the chain of sub-suppliers he intends to use

DPIA

ART. 35: The GDPR provides for a risk-based approach. It is necessary to carry out a Privacy Impact Assessment, i.e. an assessment of the risks, if it is high for the processes which involves personal data. The implementation of the technical and organizational measures (adopted or to be adopted) has to consider the analysis of the risks and costs of implementation.

Data Breach

ART. 33

In the case of an infringement of personal data (e.g. identity theft or fraud financial loss, unathorised reversal of pseudonymisation, damage to rereputation…) it is provided the obligation to notify the event and the remediation activities to the Supervisory Authority. The notification is extended to the interested party in the event that there is a high risk for the rights and freedoms of the same party.

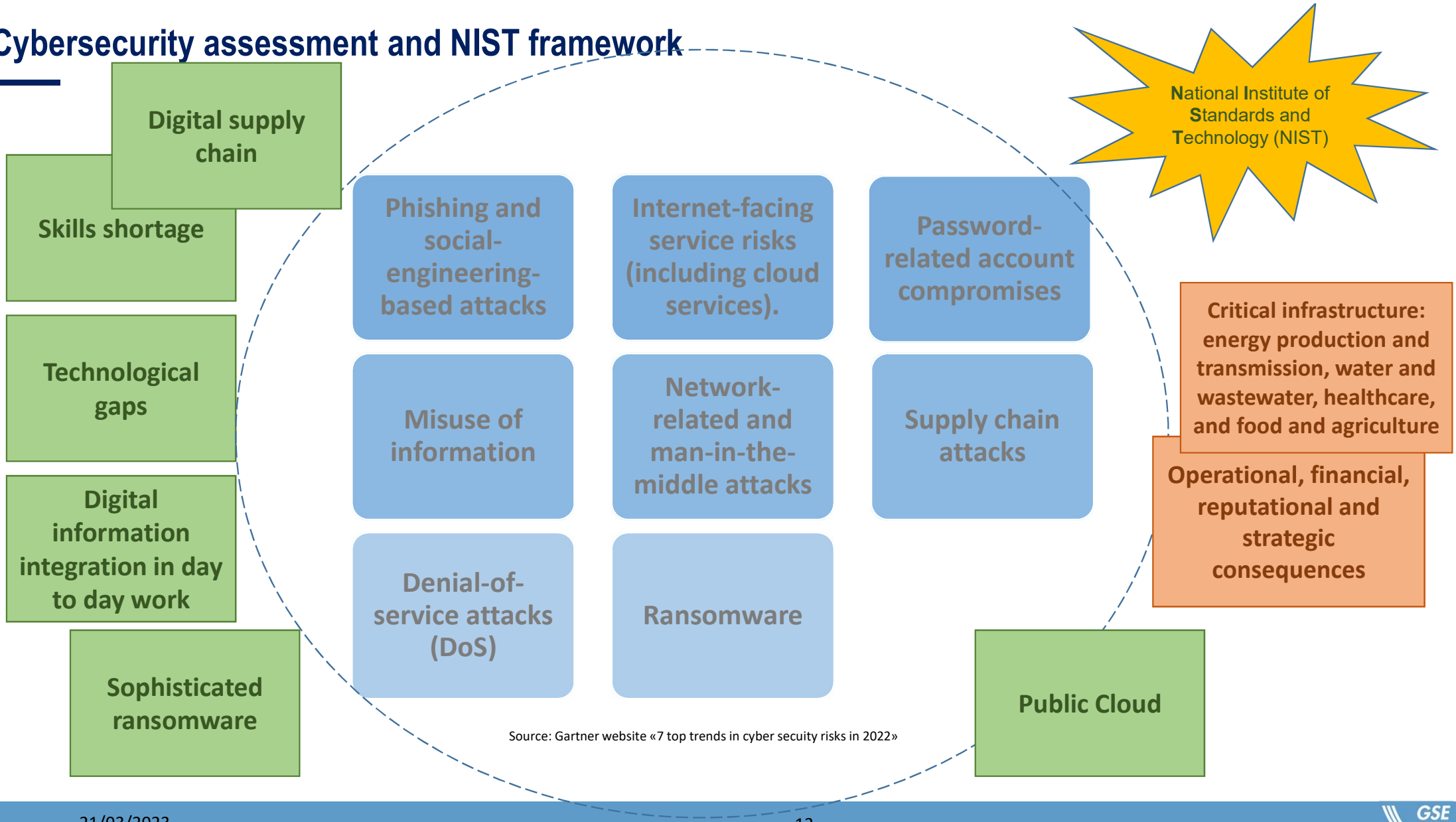
SANCTIONS

Are provided:

- **pecuniary administrative fines of up to 20 million euros / 4% of annual worldwide annual turnover;**
- **criminal sanctions in relation to offenses (e.g. unlawful data processing, unlawful communication of personal data, fraudulent acquisition of personal data; non compliance of the provisions of the control Authority…)**

There are also possible compensations of damages.

Cybersecurity assessment and NIST framework



Source: Gartner website «7 top trends in cyber secuity risks in 2022»

Cybersecurity assessment and NIST framework

National **I**nstitute of **S**tandards and **T**echnology **Cybersecurity Framework History:**

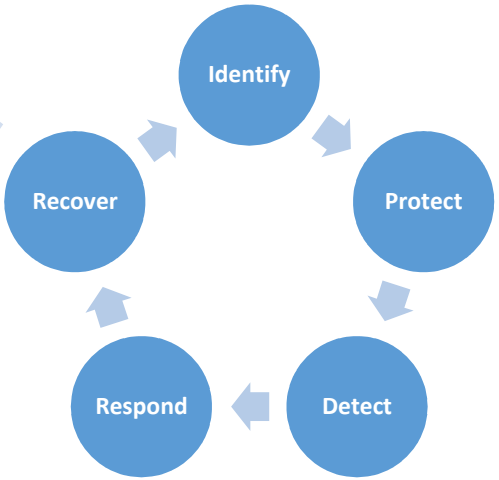
- remains effective and supports technical innovation because it is “technology neutral”

Risks and opportunities:
- increased complexity and connectivity of critical infrastructure systems
- Nation’s security, economy, and public safety and health at risk
- drive up costs and affect revenue

February 2013
Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*

December 2014
Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

May 2017
Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*



Identify, assess, and manage cyber risk

Cybersecurity assessment and NIST framework

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to: 1) Describe their current **cybersecurity posture**; 2) Describe their **target state for cybersecurity**; 3) Identify and prioritize **opportunities for improvement** within the context of a continuous and repeatable process; 4) Assess **progress** toward the target state; 5) Communicate to internal and external stakeholders about **cybersecurity risk**.

- **Core**

  Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

- **Profiles**

  Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

- **Implementation Tiers**

  A qualitative measure of organizational cybersecurity risk management practices

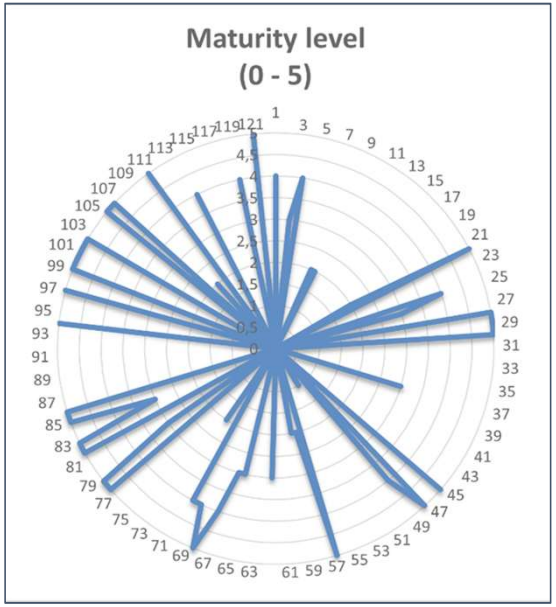
Cybersecurity assessment and NIST framework – GSE TWL project in Georgia supporting GNERC

NIST Cybersecurity Framework application in the twinning light Project GE 18 ENI EY 07 21 to assist GNERC (Georgian National Energy And Water Supply Regulatory Commission) to create enabling energy regulatory environment for digitalization in line with the terms and conditions set out in the Association Agreement and the Energy Community Treaty. Although the framework was originally intended for operators of nationally important critical infrastructure it is flexible enough to be applied to any organization or sub-unit.

To proceed with the analysis, a subset of controls was then identified for review and evaluation, according to a scale from **0 to 5** where:

- "**0-2**" implies that the controls have **not been implemented**
- "**3-4**" implies that the controls **have been partially implemented**
- "**5**" controls **fully implemented**

Of the 121 tested controls, we filtered out a set of **49 basic-level controls**, considered the minimum level to implement. It come to light that sixteen controls considered "basic" have not been implemented yet and subsequently a **priority return plan** should be defined. The result is displayed in the graph **Maturity Level**.



2G Smart Metering – regulatory framework

A decree («decreto Bersani») makes it possible to perform auctions in the field of electric power distribution starting 2025, under the condition that no operator possesses more than 25% of market

ARERA is addressing this issue similarly to gas sector, which is presently undergoing the market transition.

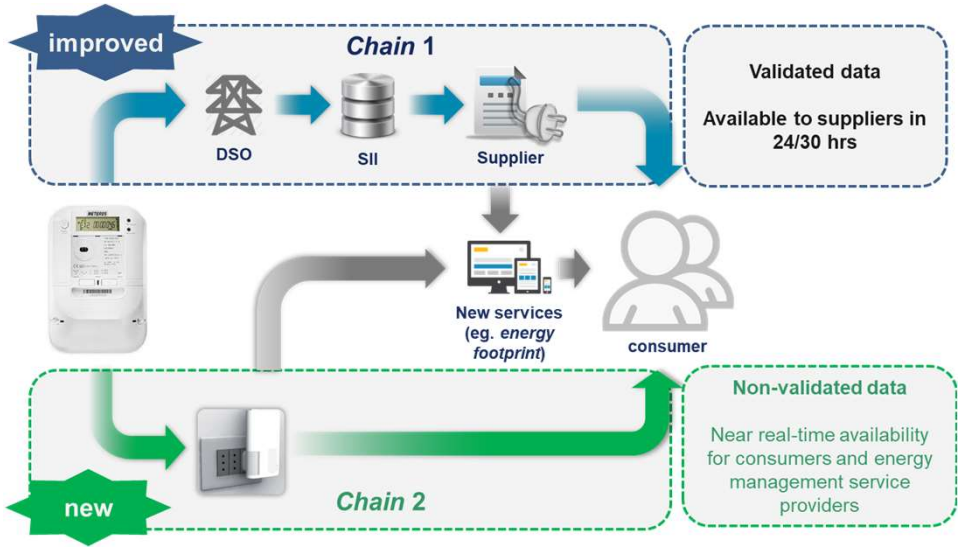
ARERA
Autorità di Regolazione per Energia Reti e Ambiente

Decision 87/2016/R/eel

- ARERA mandated CEI («Comitato Elettrotecnico Italiano») to review the proposals of DSO's and DSO associations aimed at **interchangeability** of **2G smart metering systems** in the event of a change of concession between grid operators.

2G Smart Metering - Second generation smart meters: new objectives

OBJECTIVE	MEANS
Greater efficiency of remote reading and remote control	2 embedded channels with 2 different technologies: PLC / radio frequency
Increased data granularity	Consumption of energy registered every 15' (daily curve of 96 values) and transmitted daily to DSO
Make validated data promptly available to suppliers	Consumption curves collected daily, validated by DSO and forwarded promptly to supplier through central data hub (SII)
Make data availble to consumer in near real-time	New channel to transmit near real time data (not validated) to consumers with specific device
Bi-directional communication between meter and system	Meter spontaneously sends messages to system concerning specific events (e.g. interruptions)



As defined in ARERA del. 87/2016/R/EEL

2G Smart Metering: a few definitions

Interchangeability

- ability to exchange one device by another without reducing the original functionality and without dysfunction or loss of efficiency for the whole system. Not to be confused with interoperability (CEN/CLC/ETSI/TR 50572:2011)

Interoperability

- ability of a system to exchange data with other systems of different types and/or from different manufacturers (CEN/CLC/ETSI/TR 50572:2011)

2G smart meter

- second generation meter able to sample electric measurements and to send the measurements to DSO (through chain 1) and to the client or to a party chosen by the client (through chain 2).

In order to reach **interchangeability**, a Working Group was established including a few DSO's.

The **goal** was to describe a **standard communication protocol** for **segment 1.2** between a centralized remote management system and concentrators for 2G smart meters.

The protocol description was to be so detailed that different management systems were able to manage different concentrators (provided both management systems and concentrators support the protocol).

The focus of the working group was segment 1.2 (red in figure, **see next slide**).

2G Smart Metering: standard communication protocol for segment 1.2

TECHNICAL REPORT

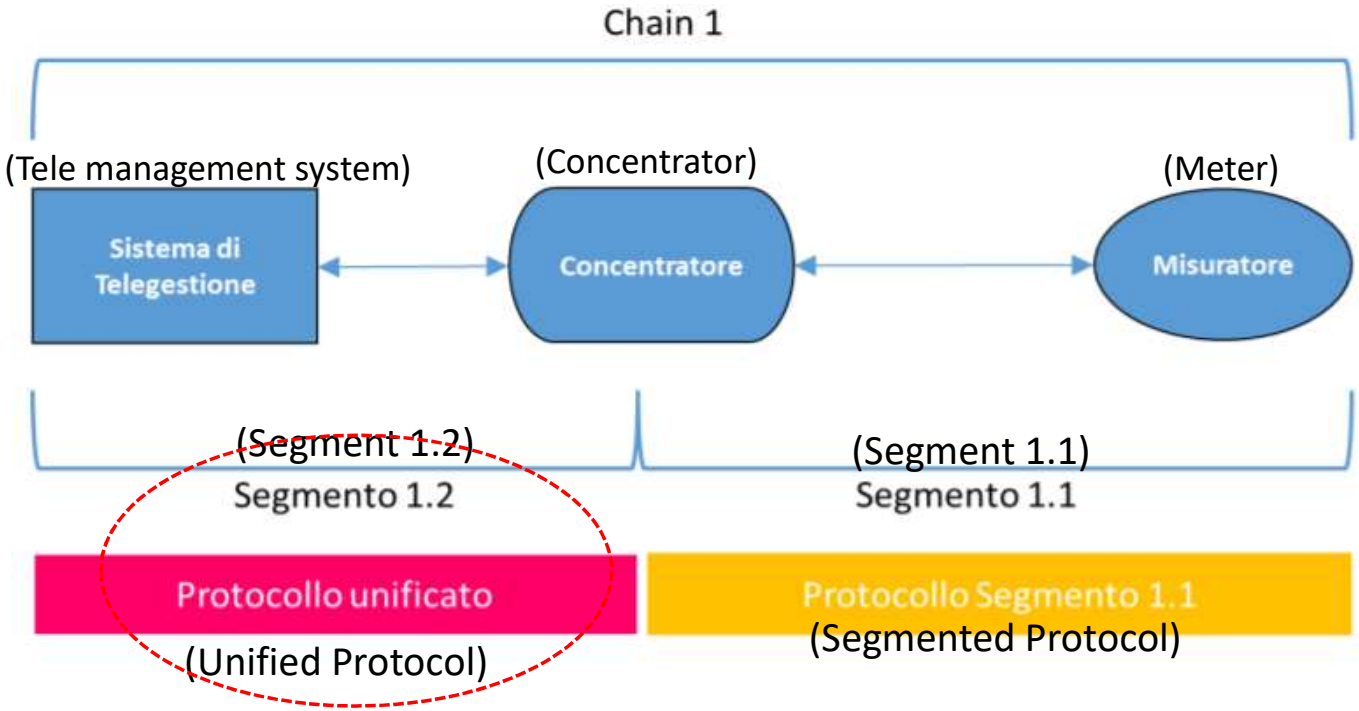
IOP_SM_2G-TR01

Interoperabilità sistemi di smart metering 2G

Ambito e Obiettivi

Gruppo di Lavoro e-distribuzione – Utilitalia

Representation of protocols for chain 1



Cybersecurity in the Smart Metering: the Italian experience

Concession take over DSO's proposal: a few steps

The incoming DSO has to connect to the concentrator and configure it

The incoming DSO provides the incumbent DSO with the new configuration parameters (APN, user, password etc.)

The incumbent DSO remotely sets the communication parameters on the concentrator

The incumbent DSO provides the incoming DSO with the safety keys of the concentrator

- Adoption of **SCEP** [Simple Certificate Enrollment Protocol].

Cybersecurity in the Smart Metering: the Italian experience

DSO's proposal

- The SCEP protocol was selected because it currently represents the de facto standard of existing implementations of PKI infrastructures
- SCEP is suitable for the specific context in which the channel of chain 1.2 is inserted, ... where the remote management system is connected to the concentrator via the telecommunications network of the distributor that manages the concentrator
- This network is owned by the aforementioned distributor and separate from the public Internet network
- EST has not been selected as it is not yet supported by all PKI infrastructure implementations, despite being among the protocols of the IEC 62351-9 specification
- EST…is particularly suitable for use on a public network, which…is not the one considered in this document
- This choice…should be periodically reviewed….The WG reserves the right to make the support of different enrollment protocols mandatory based on the evolution of the cybersecurity scenarios

Cybersecurity in the Smart Metering: the Italian experience

The take over procedure is a potential risk for interchangeability because it involves action by incumbent DSO, which has no interest in taking it. As a result, the take over might be delayed.

Proposal: each new DSO will communicate its safety keys to an independent third party (chosen by ARERA). This independent party will make them available, in due course, to the following DSO. The new communication parameters will only be activated by the new DSO..)

CEI's proposal

- Adoption of **SCEP** [Simple Certificate Enrollment Protocol] is a **potential risk** for **interchangeability** because it is suitable for a scenario where the telecommunication network is the DSO's property and is separated from the Internet. Such a scenario will certainly **disappear by 2030**.

*Proposal: abandon SCEP protocol for **EST**, which is specially suitable for use on a public network (the only scenario compatible with competition among DSO's for concessions).*

Coclusion: Take away messages

- Data security is crucial, i.a., for operation of electric distribution grids, which involves transmission of commercial and other sensible data.
- Since commerce is involved, a balance is needed between data protection and competition.
- In order to guarantee competition, it is necessary (although not sufficient) to make transition between DSO's possible.
- The intervention of an independent third party is needed, so that no DSO can hinder transition.
- When it comes to technological choices (like that of certificate management protocols), the possibility of transition should be regarded as a major driver.

THANK YOU FOR YOUR KIND ATTENTION

THE ENERGY
OF THE PRESENT


CISA Certified Information Systems Auditor.
An ISACA® Certification

ISACA hereby certifies that

Dr. Pietro Falconi CISA,CISM

has successfully met all requirements and is qualified as a Certified Information Systems Auditor; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

Certificate Number	Date of Certification	Expiration Date
CISA-0544223	17 November 2005	31 January 2024

ISACA

ISACA Chief Executive Officer


CISM Certified Information Security Manager.
An ISACA® Certification

ISACA hereby certifies that

Dr. Pietro Falconi CISA,CISM

has successfully met all requirements and is qualified as a Certified Information Security Manager; in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISM continuing professional education policy; and passage of the CISM exam.

Certificate Number	Date of Certification	Expiration Date
CISM-1014150	28 June 2010	31 January 2026

ISACA

ISACA Chief Executive Officer

Contacts:

- pietro.falconi@gse.it
- giuseppedellolio@gse.it