D1.1 European Disruption Resilience Snapshot

Submission date: 30th of June 2025

Due date: 30th of June 2025

Version 1.0

DOCUMENT SUMMARY INFORMATION

Grant Agreement No	101168007		
Full Title	Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe		
Start Date	01/10/2024	**Duration**	36 months
Deliverable	D1.1 European Disruption Resilience Snapshot		
Work Package	WP1 – COOPERATION: Strategic Collaboration & Cooperation (Phase 1)		
Type	R	**Dissemination Level**	PU
Lead Beneficiary	ICS		

Table 1: List of changes

Version nr.	Date	Change	Author
0.1	13.01.2025	Initial draft ToC	Denis Caleta, Aljosa Kandzic
0.2	23.05.2025	Initial draft of report	Denis Caleta, Aljosa Kandzic
0.3	05.06.2025	Final draft ready for peer review	Denis Caleta, Aljosa Kandzic
0.4	14.06.2025	Peer review (DNSC)	Cristian Nistor, Radu Dumitru, Andreea Scarlat, Daniela Tapi
0.4	16.06.2025	Peer review (URSIV)	Marjan Kavcic
0.5	25.06.2025	Peer review comments addressed	Denis Caleta, Aljosa Kandzic
0.6	27.06.2025	Pre-final version	Denis Caleta, Aljosa Kandzic
0.7	30.06.2025	SAB review	Gabriele Giunta, Adelin-Marian Homoraceanu
0.8	30.06.2025	QA review	Liana-Miruna Predut, Ioana-Andreea Craciun
1.0	30.06.2025	Final version	Denis Caleta, Aljosa Kandzic

Table 2: Contributors

Entity Short Name	Contributor name
INS	Gilda De Marco
TLX	Hans Graux
TLX	Krzysztof Garstka
EVIDEN-RO	Liana-Miruna Predut
EVIDEN-RO	Adelin-Marian Homoraceanu
SYN	Emmanouil Mavrogiorgis

Table of Contents

Acronyms and Abbreviations

Acronyms

Acronym	Description
AI	Artificial Intelligence
CER	Critical Entity Resilience
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CER	Critical Entity Resilience
CIR	Critical Infrastructure Resilience
EC	European Commission
ENTSO-E	European Network of Transmission System Operators for Electricity
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
EU WS	EU workshop
ESP	Essential Service Providers
FAIR	Findable, Accessible, Interoperable, and Reusable
IP	Intellectual Property
IPR	Intellectual Property Rights
IR	Internal Reviewer
ML	Machine Learning
MS	Member States
NRA	National Risk Assessment
NIS	Network and Information Security Directive
PC	Project Coordinator
PO	Project Officer
SAB	Security Advisory Board
SEN	Sensitive
TL	Task Leader
TM	Technical Manager
WP	Work package
WPL	Work package Leader
WS	Workshop

Abbreviations

Abbreviation	Description
N/A	

List of Figures

Executive summary

This deliverable represents a key component of Work Package (WP1), which ensures effective and in-depth analysis and foundational understanding of the functioning of critical infrastructure (CI) stakeholders across the European Union, including competent authorities, operators, and other actors involved in essential services provision. It explores both the strategic and operational mechanisms for cross-sector and cross-border collaboration and cooperation, with particular focus on enhancing resilience within and across critical sectors and EU member states.

WP1 activities are structured around two interrelated objectives: (1) to collect targeted insights from CI stakeholders to inform the work of subsequent work packages (WP3–WP8); and (2) to explore, define, and test improved models of collaboration and cooperation (WP9). The knowledge generated—rooted in both challenges and best practices will shape shared understanding of the current state of CI resilience and provide a basis for more effective, coordinated strategies.

Based on the outcomes of these efforts, we identified and analyzed key gaps in existing regulatory and operational frameworks and defined concrete use cases to guide the development and evaluation of the ENDURANCE strategy and services.

1 Introduction

This deliverable represents a key component of Work Package (WP1), which ensures effective and in-depth analysis and foundational understanding of the functioning of critical infrastructure (CI) stakeholders across the European Union, including competent authorities, operators, and other actors involved in essential services provision. It explores both the strategic and operational mechanisms for cross-sector and cross-border collaboration and cooperation, with particular focus on enhancing resilience within and across critical sectors and EU member states.

WP1 activities are structured around two interrelated objectives: (1) to collect targeted insights from CI stakeholders to inform the work of subsequent work packages (WP3–WP8); and (2) to explore, define, and test improved models of collaboration and cooperation (WP9). The generated knowledge — rooted in both challenges and best practices will shape the shared understanding of the current state of CI resilience and provide a basis for more effective, coordinated strategies.

To support these objectives, a dedicated Pan European Working Group on Disruption Resilience (WGDR) has been established, composed of relevant networks and individual experts drawn from the project consortium as well as external stakeholders representing sectors and countries not directly involved in the consortium. This Working Group will play a central role in informing the project by participating in structured consultations and engaging in iterative evaluation of the project's results.

The first phase of WP1 (until Month 9 - July 2025) concentrates on establishing this Working Group and assessing current definitions, methodologies, and practices related to critical entity resilience (CER)—including the definition of essential services, identification of critical entities, and approaches to risk assessment, interdependencies, and cascading effects. Data for this phase was gathered through desk research, expert surveys (where applicable), and a series of local national workshops (WL1) conducted in the pilot countries: Slovenia, Romania, Italy, and Greece. The workshops were organized during the first three months to facilitate direct engagement with CI stakeholders and gather insights on operational challenges and successful practices. A broader European-level workshop (WE1) was scheduled in Month 6 to support cross-border exchange and reinforce the findings from national-level consultations. The workshops served for strengthening relationships among the CI stakeholders, exchanging knowledge, experience, and best practices among them, and gathering inputs for the development and co-creation of the ENDURANCE results. Enhanced strategic cooperation, active collaboration, and continuous communication among the CI stakeholders enabled faster identification of potential challenges and gaps, and faster identification of effective solutions and coordinated actions for better joint resilience against disruptions.

Based on the outcomes of these efforts, we identified and analyzed key gaps in the existing regulatory and operational frameworks and defined concrete use cases to guide the development and evaluation of the ENDURANCE strategy and services. These findings, as presented in this report, provide the initial building blocks for an evidence-based, user-informed approach aimed at improving the resilience of critical infrastructures in Europe.

2 Analysis of current practices and gaps for critical infrastructure resilience

2.1 Analysis of existing strategy, policy and doctrine documents

This chapter provides a detailed analysis of existing strategy, policy and doctrine documents related to disruption and business continuity of critical entities. The resilience of critical entities, particularly in the context of disruptions caused by natural disasters, cyber incidents, hybrid threats, or systemic failures, relies heavily on the strategic, policy, and doctrinal frameworks that guide preparedness, response, recovery, and continuity planning. This section presents a comprehensive analysis of existing documents at national and EU levels that shape how CI operators prepare for and manage continuity in the face of disruption.

2.1.1 Strategic Frameworks

At the EU level, the EU Critical Entities Resilience (CER) Directive forms the core strategic instrument aimed at enhancing the resilience of entities operating in essential service sectors. The Directive mandates Member States (MS) to identify critical entities, conduct risk assessments, and ensure that those entities develop and implement appropriate resilience and business continuity plans. The directive builds upon previous frameworks, such as the European Programme for Critical Infrastructure Protection (EPCIP) and aligns with broader EU resilience goals under the Union Civil Protection Mechanism and the EU Security Union Strategy.

National strategies, although aligned with EU directives, vary significantly in scope and maturity. Many MS have developed national resilience or critical infrastructure protection strategies that address sector-specific threats, interdependencies, and incident response coordination. However, notable gaps exist in the integration of new risk vectors such as cyber-physical convergence, climate change, or geopolitical hybridization.

2.1.2 Policy Instruments and Operational Guidelines

Policies related to business continuity and disruption response often reside within civil protection and cybersecurity domains. For instance, National Risk Assessment (NRA) documents commonly include risk scenarios and business impact analyses that feed into sectoral emergency planning. Additionally, sector-specific regulations, such as those in energy, health, finance, and transport, impose continuity obligations on operators, though these are unevenly defined and enforced.

A recurring issue in policy implementation is the fragmented nature of requirements across sectors. For example, while energy and financial sectors typically have well-defined business continuity protocols under EU-level supervision (e.g., through the European Network of Transmission System Operators for Electricity (ENTSO-E)[1] or the European Central Bank), other sectors such as water supply or digital services may lack binding continuity standards or doctrinal support.

Furthermore, policies often focus on compliance and planning rather than continuous adaptation and learning. This limits their ability to respond to complex, evolving threat environments. This gap

[1] ENTSO-E https://www.entsoe.eu/

between static policy frameworks and dynamic threat landscapes represents a significant challenge for maintaining effective critical infrastructure resilience.

2.1.3 Doctrine and Practice

Doctrinal documents such as national emergency management doctrines, military-civil cooperation manuals, and cybersecurity incident response protocols define the practical implementation of resilience and continuity strategies. These documents are instrumental in defining inter-agency roles, standard operating procedures, and escalation mechanisms during disruptive events.

However, the doctrinal landscape is often siloed. Insufficient doctrinal integration exists across domains (e.g., cybersecurity, physical security, supply chain resilience), and there is limited emphasis on holistic, all-hazard approaches. Moreover, simulation-based validation of doctrines through joint exercises, red-teaming, or war-gaming is not consistently applied across MS.

2.2 EU legislation governing critical entity (CE) resilience

This subsection explores the key EU-level legislative instruments for enhancing the resilience of critical infrastructure. These instruments include both Regulations (directly applicable law across Member States) and Directives (requiring national transposition to become operational). These laws apply to different entities, sectors, and activities, each supporting resilience in a different way. The following graphic presents their targeted actors and/or regulated activities in the context of the ENDURANCE project. Each instrument is then described in a dedicated subsection, with the CER Directive and Network and Information Systems 2 (NIS2) Directive receiving particular attention due to their high relevance.

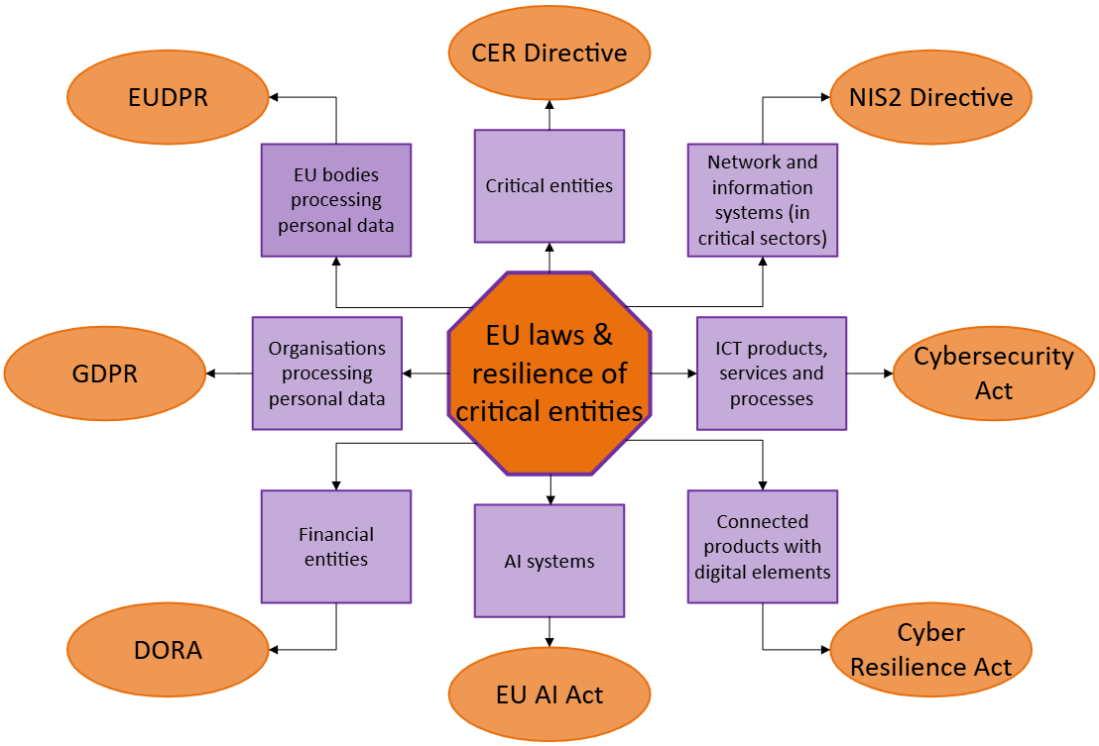


Figure 1: Scheme of EU legal framework.

Directive 2022/2557 – Critical Entities Resilience Directive (CER Directive)[2]

The CER Directive is a crucial legislative instrument in the EU's drive to improve the resilience of services that are "essential for the maintenance of vital societal functions or economic activities".[2] It seeks to enhance, broaden, and harmonize MS' efforts in this regard.

The Directive was adopted on 14 December 2022 and entered into force on 16 January 2023, with a MS transposition deadline of 17 October 2024. Simultaneously, the instrument's regulatory framework is set to become fully operational after 17 July 2026.

The Directive was initiated to deal with an evolving landscape of threats to critical services, characterized by factors such as global pandemic, geopolitical tensions and natural disasters. The Nord Stream pipeline explosion exemplifies such a threat, expressly cited by the European Commission (EC).[3] The increasingly interconnected nature of critical services acted as a catalyst in this regard. Additionally, the CER Directive builds on and replaces an earlier instrument on critical infrastructure, Directive 2008/114.[4]

The Directive seeks to cover both public and private entities from eleven core sectors. These sectors include:

Energy – Transport – Banking – Financial market infrastructure – Health – Drinking water – Wastewater – Digital infrastructure – Public administration – Space - Production, processing and distribution of food

Using a non-exhaustive list provided by the European Commission (EC),[5] MS has to identify specific CE by 17 July 2026, which will then be subjected to dedicated obligations set out in the Directive. The process for identifying such entities can be summarized in three steps: (1) the entity must provide an essential service; (2) it must operate on the territory of that MS and locate its critical infrastructure there; and (3) an incident involving it would have "significant disruptive effects" on the provision of essential services (by this entity or another).[6] Some of these entities may also be classified as "critical entities of particular European significance", where they provide the same or similar services in six or more Member States.[7]

Core pillars of the CER Directive are:

- *National resilience strategies – MS must define and adopt a strategy for enhancing the resilience of critical entities, by 17 January 2026. This strategy must contain elements such as strategic objectives and priorities; governance framework; necessary resilience measures; the process for identifying CE; and a list of actors involved in implementing the strategy*.[8]
- *Risk assessment (MS level)* – Every four years, MS must conduct a risk assessment that will serve as a key reference point for identification of CEs by the national, competent authorities.

[2] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L333/164 (CER Directive).
[3] See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992.
[4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[5] Implementing Act (Commission Delegated Regulation (EU) 2023/2450 of 25 July 2023).
[6] CER Directive, fn. 2 art. 6.
[7] CER Directive, fn. 2 art. 17.
[8] CER Directive, fn. 2 art. 4.

Risks considered ought to be of both natural and man-made character, including cross-sectoral and cross-border ones.[9]

- *General support to CEs* – MS must provide support to CE, aimed at enhancing their resilience. This might take the form of guidance materials and methodologies, facilitated testing exercises, advice, and training. Where necessary and justified, financial resources may also be provided.[10]
- *Risk assessment (CE level)* – After being identified as a CE (and at least every four years thereafter), CE must conduct a risk assessment, focused on risks that could disrupt their provision of essential services. This assessment should follow the MS-level risk assessment in covering both natural and man-made risks, including cross-border and cross-sectoral ones, as well as considering the impact on other essential services.
- *Measures to be taken by the CE* – MS must ensure that (following both levels of risk assessment), the CE take suitable technical, security and organizational measures, necessary to: prevent incidents; respond to them appropriately if they happen; recover from them; ensure physical protection of premises and infrastructure; manage employee security and raise internal awareness.[11] Additionally, CE have the option of requesting background checks from public authorities.[12]
- *Competent authorities* – MS must designate or establish competent authorities that will be responsible for the correct application and enforcement of the Directive. These authorities are to carry out MS-level risk assessments, identify specific CE, conduct inspections, facilitate the sharing of knowledge and good practices with and among CE, request information from CE, process incident notifications, and impose penalties for non-compliance.[13]

The CER Directive is a cornerstone of the EU's regulatory response aimed at enhancing the resilience of the Union's critical entities, addressing their needs directly. At the time of writing, its impact is too early to assess; however, the EC's proposed list of essential entities is available[14] and MS have until 17 January 2026 to develop their national strategies; both being good anchor points for feedback and contribution in this field.

[9] CER Directive, fn. 2 art. 5.
[10] CER Directive, fn. 2 art. 10.
[11] CER Directive, fn. 2 art. 13.
[12] CER Directive, fn. 2 art. 14.
[13] CER Directive, fn. 2 art. 9.
[14] See https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992.

Directive 2022/2555 – NIS2 Directive[15]

While the CER Directive focuses on general resilience of critical entities, the related NIS2 Directive concentrates on cybersecurity in the context of network and information systems functioning in the EU's critical sectors. In this way, it seeks to contribute to a "high common level of cybersecurity across the Union".[16] The two instruments are considered complementary to each other.

The Directive was adopted on 14 December 2022, entered into force on 16 January 2023, with a national transposition deadline of 17 October 2024; same as the CER Directive.

As the numbering suggests - the NIS2 Directive builds on and replaces an earlier instrument on critical infrastructure, the NIS (1) Directive.[17] The challenges that triggered the need for a legislative update start with the fragmented approach amongst MS. For instance, some of them designated certain hospitals as essential entities, while others did not. Moreover, NIS1 covered a limited number of sectors and its information sharing objectives were not successfully implemented in practice. Additionally, enforcement mechanisms were perceived to be relatively weak.[18]

The NIS2 Directive focuses on essential and important entities, these terms relate to the role played by the services they operate (with essential entities being subjected to more stringent requirements). To this end, the Directive identifies 18 sectors, dividing them on 11 sectors of high criticality, and 7 sectors of lesser criticality:[19]

Energy – Transport – Banking – Financial market infrastructures – Health – Drinking water – Wastewater – Digital infrastructure – ICT service management (business-to-business) – Public administration - Space

And 7 other critical sectors:[20]

Postal and courier services – Waste management - Manufacture, production and distribution of chemicals - Production, processing and distribution of food – Manufacturing - Digital providers - Research

These sectors serve as a key reference point for MS in identifying essential and important entities; a list they had to complete by 17 April 2025 and must update every two years.[21] Key criteria that MS must consider in this regard include: (1) role in maintaining critical societal or economic activities; (2) impact of service disruption on public safety, security or health; (3) disruption-related creation of a systemic (especially cross-border) risk.[22]

[15] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L333/80.
[16] NIS2 Directive, fn. 15, art. 1.
[17] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.
[18] For further coverage of the NIS2 Directive, see this blog post by Niels Vandezande https://www.timelex.eu/en/blog/re-newing-eus-cybersecurity-strategy-nis2.
[19] NIS2 Directive, fn. 15, Annex 1.
[20] NIS2 Directive, fn. 15, Annex 2.
[21] NIS2 Directive, fn. 15, art. 3(3).
[22] NIS2 Directive, fn. 15, art. 2(2).

Additionally, such entities may be public or private, and they are predominantly larger organizations (though a pathway exists for including crucial SMEs and micro-SMEs in the scope of the Directive).

The core pillars of the NIS2 Directive are:

- *National cybersecurity strategies* – MS must adopt these strategies, and ensure they include: objectives and priorities (particularly for the 18 identified sectors); governance frameworks; risk assessment and response mechanisms; a list of key related authorities and stakeholders; and a plan for cybersecurity awareness among citizens. Specific attention has to be paid to aspects such as supply chain security, requirements for ICT products and services, as well as managing vulnerabilities.[23] These strategies are to be reviewed at least every five years.
- *Authorities* – MS must designate or establish a set of authorities to reinforce the Directive's goals, namely: competent authorities for cybersecurity and supervision of the Directive's implementation, single points of contact, cyber crisis management authorities and computer security incident response teams (CSIRTs).
- *Collaboration* – At both national and Union levels, the Directive contains multiple provisions aimed at improving collaboration among the indicated authorities and other stakeholders. This covers both short-term initiatives (such as incident response) and long-term ones (such as knowledge and best practice sharing). Specific initiatives established by the Directive include a CSIRTs network[24] and the European cyber crisis liaison organization network (EU Cyclone).[25]
- *Cybersecurity requirements for essential and important entities* - These include an increased role of management bodies in cybersecurity; risk assessment and management duties; and use of suitable technical, operational and organizational measures. The minimum package of these measures is to include elements such as policies (for risk analysis and information system security), incident handling measures, supply chain security measures and more.[26] For incident handling specifically, it is important to highlight the chain of reporting obligations towards CSIRTs/competent authorities, which are set at maximum of 24 hours from discovery (first notification), 72 hours (initial assessment) and one month from the initial notification (for a more detailed response report).[27]
- *Enforcement and supervision* – MS must ensure that competent authorities under the Directive are able to enforce and supervise its implementation, including through direct interactions with essential and important entities. Powers available to authorities include on-site inspections, security audits and scans, as well as requests for information, data and evidence.[28]

The NIS2 Directive is highly relevant to the resilience of critical entities, as it governs their response towards cybersecurity concerns. Notably, it works in tandem with the CER Directive; as recital 30 of

[23] NIS2 Directive, fn. 15, art. 7.
[24] NIS2 Directive, fn. 15, art. 15.
[25] NIS2 Directive, fn. 15, art. 16.
[26] NIS2 Directive, fn. 15, art. 21.
[27] NIS2 Directive, fn. 15, art. 23. Also, for more details, see this blog post by Bernd Fiten and Wout Platteau https://www.timelex.eu/en/blog/24-hours-72-hours-1-month-reporting-cyber-incidents-under-nis2.
[28] NIS2 Directive, fn. 15, arts. 32 and 33.

NIS2 states, “in view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured” (between the two Directives). This approach is visible in the statement that critical entities under the CER Directive are to be considered essential entities within the NIS2 Directive.[29]

Regulation 2019/881 – EU Cybersecurity Act[30]

The EU Cybersecurity Act was enacted to strengthen the European Union's cybersecurity framework by granting the EU Agency for Cybersecurity (ENISA) a permanent mandate and establishing a European cybersecurity certification framework for information and communications technology (ICT) products, services, and processes.

The Act was adopted on 17 April 2019 and entered into force on 27 June 2019. It emerged in response to the EU’s desire to assume a more central position in ensuring a harmonized and effective approach to cybersecurity at the EU level.

Regarding ENISA, the EU Cybersecurity Act establishes its role as a center of expertise on cybersecurity, assisting the EU and its Member States in matters of cybersecurity policy, improving capacity-building and preparedness; facilitating cooperation between different actors and countries; contributing to Union law and policy; and more.[31]

Regarding the cybersecurity certification framework, the Act seeks to promote it, to support the creation of a digital single market for ICT products, services and processes. Specific security objectives that any certification scheme established under the framework should achieve include protection of data during the entire lifecycle of the ICT product, service or process; access rights; dependencies and vulnerabilities; and records.[32]

By enhancing ENISA's role in supporting Member States with expertise and facilitating coordinated responses to cyber threats, the Act contributes significantly to the resilience of critical entities and infrastructure. For example, ENISA features prominently as a meaningful actor in the NIS2 Directive. Additionally, the certification framework promotes consistent security standards across the EU, ensuring that ICT products and services integral to essential operations meet robust cybersecurity requirements. This thereby bolsters the overall resilience of critical entities.

[29] NIS2 Directive, fn. 15, rec 30.
[30] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.
[31] EU Cybersecurity Act, fn. 30, arts. 4 and 5.
[32] EU Cybersecurity Act, fn. 30, art. 51.

Regulation 2024/2847 - Cyber Resilience Act[33]

The Cyber Resilience Act (CRA) aims to enhance cybersecurity across the EU by establishing common standards for products with digital elements (both hardware and software), that are available on the market and used to connect to a device or network.

The Act was adopted on 23 October 2024 and entered into force on 10 December 2024.

A core motivation for the passage of the Act was to ensure security-by-design of Internet of Things (IoT) devices. By mandating that such products are designed, developed, and maintained with appropriate cybersecurity measures throughout their lifecycles, the CRA seeks to reduce vulnerabilities and ensure timely security updates.

The CRA's regulatory approach rests on four pillars:[34]

- Rules for making products available on the market.
- Cybersecurity requirements (for design, development and production).
- Cybersecurity requirements (for vulnerability handling).
- Market surveillance.

The CRA is relevant to the resilience of critical entities and infrastructure, as it ensures that the digital products integral to essential services (including IoT devices) possess robust security features. This approach mitigates risks associated with cyber threats and enhances the overall stability and security of critical entities within the EU.

Regulation 2024/1689 – Artificial Intelligence Act (EU AI Act)[35]

The EU AI Act is the EU's chief legal instrument for regulating the development, implementation and deployment of AI technologies.

The Act was adopted on 13 June 2024 and entered into force on 1 August 2024.

The Act establishes a risk-based regulatory framework for AI systems, categorizing them by potential harm levels, with a ban on certain uses of AI and stringent requirements for high-risk AI systems. This includes those used in critical infrastructure sectors such as energy, transport, and healthcare.

By mandating robust risk management, transparency, and security measures, the Act seeks to ensure that AI systems integrated into essential services are resilient against disruptions and cyber threats. This regulatory approach enhances the overall resilience of critical entities by promoting the development and deployment of trustworthy and secure AI technologies.

[33] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L2847/1.
[34] Cyber Resilience Act, fn. 33, art. 1.
[35] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689.

Regulation 2022/2554 - Digital Operational Resilience Act (DORA)[36]

DORA is an EU Regulation enacted to bolster the digital operational resilience of financial entities.

DORA was adopted on 14 December 2022 and entered into force on 16 January 2023. Its provisions apply from 17 January 2025.

The Regulation mandates that financial institutions (21 different types, including banks, insurance companies, and investment firms) implement comprehensive frameworks for managing information and communication technology (ICT) risks. This includes stringent requirements for risk management, incident reporting, resilience testing, and oversight of third-party ICT service providers.

By establishing uniform standards across the EU financial sector, DORA addresses critical financial services, enhancing their readiness to prevent, respond to, and recover from ICT-related disruptions. This approach strengthens the overall resilience of critical infrastructure within the Union, particularly within the financial market infrastructure sector regulated by the CER Directive.

Regulation 2016/679 - General Data Protection Regulation (GDPR)[37]

GDPR establishes a comprehensive framework for the protection of personal data within the European Union.

The GDPR was adopted on 27 April 2016, entered into force on 24 May 2016, and its provisions become available from 25 May 2018.

While primarily focused on data privacy and individual rights, the GDPR holds significant implications for the resilience of critical entities and infrastructure. By mandating robust data governance, breach notification protocols, and security measures, the GDPR contributes to the operational integrity and cybersecurity of essential services. Therefore, compliance with the GDPR enhances the overall resilience of critical infrastructure by reducing vulnerabilities related to data misuse, cyber threats, and system disruptions.

Regulation 2018/1725 - Data Protection Regulation for EU institutions, bodies, offices and agencies (EUDPR)[38]

The EUDPR governs the processing of personal data by EU institutions, bodies, offices, and agencies, aligning closely with the principles of the GDPR. Adopted to ensure high standards of data protection

[36] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 [2022] OJ L333/1.
[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[38] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.

within EU entities, the EUDPR mandates strict safeguards, accountability mechanisms, and incident response procedures.

The EUDPR was adopted on 23 October 2018 and entered into force on 11 December 2018.

Similar to the GDPR, its relevance to the resilience of critical entities and infrastructure lies in its emphasis on data security and risk management. By enforcing stringent data protection requirements, the EUDPR supports the continuity and trustworthiness of operations within critical EU institutions. These institutions often play key roles in EU-wide resilience, such as ENISA or the EU AI Office This approach thereby contributes to the broader resilience and security framework of essential services across the Union.

2.3 Gaps and Opportunities related to Analysis of existing strategy, policy and doctrine documents

Our analysis identifies several key gaps in the current strategic and policy architecture:

- **Lack of harmonization** in business continuity expectations across Member States and sectors.
- **Limited integration** of resilience concepts into procurement, governance, and long-term strategic planning.
- **Insufficient use of real-time data** and AI-supported decision systems in continuity planning.
- **Underutilization of public-private partnerships** in both planning and operational response to disruptions.
- **Deficient feedback loops** from incident after-action reviews into policy updates and doctrinal improvements.

Recommendations

To enhance the effectiveness of disruption management and business continuity frameworks for critical entities, the following actions are recommended:

1. **Harmonize and update national strategies** to align with CER Directive requirements and integrate cross-sectoral resilience principles.
2. **Develop interoperable continuity doctrine**, supported by common standards, playbooks, and joint training for public and private stakeholders.
3. **Incentivize the adoption of digital twins, predictive analytics, and real-time monitoring** to support continuity-of-operations decision-making.
4. **Foster cross-border collaboration mechanisms** for continuity planning, especially for entities operating in transnational critical infrastructures.

5. **Establish national and EU-level resilience observatories** to systematically monitor policy implementation, document best practices, and guide iterative updates to strategy and doctrine.

2.4 Analysis of existing lessons learned for providing resilience from past crisis situations

In recent years, numerous events ranging from cyber-attacks to natural disasters have triggered crisis situations, compromised the functionality of essential services and highlighted vulnerabilities within critical services networks. These demonstrate that current security and prevention measures are no longer sufficient to ensure the operational continuity of essential services. Resilience can no longer be viewed only as the ability to quickly recover from an adverse event, it must also include the ability to anticipate, withstand, and adapt to a wide range of threats. This requires an integrated approach that combines advanced technologies, improved risk management practices, and a culture of prevention and investment in resilience.

Investing in resilience means protecting society, the economy, and national security, while ensuring that critical infrastructures can withstand, adapt, and quickly recover from any type of crisis. Achieving this goal requires analyzing and understanding the variability of the concept of resilience and the factors that affect it, such as the type of threats, geographical context, sector, technology, interdependencies, etc. One of the main resources to be prepared to this new challenge is **learning from the past**, both in terms of events and studies.

Past events are fundamental to improving resilience; every crisis provides valuable information that can be used to enhance future strategies. These lessons learned must guide the planning and implementation of resilience strategies, to capitalize on good practices and avoid repeating past mistakes.

The analysis of lessons learned from past crisis situations reveals critical insights into enhancing resilience for future emergencies. Historical analysis of crises, such as natural disasters, pandemics, and cyber-attacks, has underscored the importance of preparedness, communication, and adaptability in building resilient systems.

The following crisis situations that occurred in Europe over the past five years illustrate key considerations for improving resilience at both ecosystem and entity levels:

- **Widespread Blackout Across Iberia (2025):** On 28 April 2025, the Iberian Peninsula experienced one of its most severe power outages. At 12:33 CEST, a series of generation trips occurred in southern Spain, leading to a loss of 2,200 MW in generation capacity. This caused a significant frequency to drop below 48.0 Hz, triggering automatic load shedding and the tripping of AC lines between France and Spain. The grid collapsed completely, and the HVDC interconnection between France and Spain also tripped. The resulting blackout affected mainland Portugal, peninsular Spain, Andorra, and parts of southwest France, with power interruptions lasting about ten hours in most of the Peninsula and longer in some areas. The outage caused severe disruptions in telecommunications, transportation systems, and essential services. At least seven people in Spain and one in Portugal died due to outage-

related circumstances. The total disconnected load was estimated at 30 GW. Restoration efforts involved black start procedures from hydro and gas power stations. Portugal's grid was fully restored by 00:22 CEST on 29 April, while Spain's grid achieved full restoration by 04:00 CEST.[39] The exact cause of the blackout remains under investigation. Preliminary analyses suggest that the outage was triggered by a physical infrastructure failure—specifically, a fault on a critical transmission line, possibly due to an external event such as a fire.[40]

- **Flood in Valencia (2024)**: It highlighted the importance of early warning systems for promptly alerting populations and reducing casualties. The events demonstrated the critical need to review water resource management and infrastructure maintenance to prevent catastrophic damage.
- **Cyber-attack in Italy (2024)**: The pro-Russian group Noname057 launched a series of DDoS attacks against institutional and corporate websites, including the Ministry of Foreign Affairs, Milan airports (Linate and Malpensa), and the online system of Banca Intesa Sanpaolo.
- **Flood in Slovenia (2023):** Violent flash floods caused extensive damage to infrastructure, including buildings, roads, and electrical networks. These events emphasized the need for improved land management and enhanced coordination and communication among crisis management actors.
- **Wildfires in Portugal (2022):** These fires demonstrated the need for more effective prevention strategies, such as forest management and firebreak creation, while highlighting the importance rapid, coordinated emergency service response to contain fires and reduce damage.
- **Cyber-attack on the power grid in Ukraine (2022)**: This attack underscored the importance of strengthening cyber resilience of critical infrastructures to prevent and mitigate cyber-attack effects. Continuous training and awareness of cyber threats are pillars for protecting infrastructures and responding effectively to attacks.
- **Interconnector Failure and Grid Separation (2021)**
    - On 24 July 2021, a major incident led to the temporary separation of the Iberian Peninsula from the Continental European power system. The event was triggered by the tripping of the 400 kV Baixas–Gaudière 2 line at 16:33:12 CEST, followed by the Baixas–Gaudière 1 line at 16:35:23.8 CEST. These failures caused a significant voltage phase angle to increase between France and Spain, leading to system instability and the disconnection of the Iberian grid from the rest of Europe.[41]
    - The incident resulted in the loss of approximately 2,350 MW of electricity supply in Spain and around 1,000 MW in Portugal. Power was restored within an hour, with the first interconnection line with France re-energized 36 minutes after the incident, and full supply recovery achieved by 17:38 CEST. [42] An expert panel comprising ENTSO-E,

[39] Brezar, Aleksandar (28 April 2025). "Breaking news. Spain, Portugal and southern France hit by massive power outage". *Euronews*. Archived from the original on 28 April 2025. Retrieved 28 April 2025.
[40] Ferris, Nick (30 April 2025). "Did Spain's push for renewable energy have any impact on its mass power blackout?". *The Independent*. Retrieved 3 May 2025.
[41] Final report on the power system separation of Iberia from Continental Europe on 24 July 2021, https://www.entsoe.eu/news/2022/03/28/final-report-on-the-power-system-separation-of-iberia-from-continental-europe-on-24-july-2021/?utm_source=chatgpt.com
[42] Interconnector Failure in France Causes Outages Across Iberian Peninsula (2021). https://www.theblackoutreport.co.uk/2021/07/26/interconnector-failure-iberian-peninsular-blackout/?utm_source=chatgpt.com

relevant Transmission System Operators (TSOs), and regulatory authorities conducted a comprehensive investigation into the incident. The final report emphasized the importance of avoiding the tripping of generation connected to distribution systems to maintain system security.[43]

- **Floods in Germany and Belgium (2021)** showcased the importance of infrastructure resilience and rapid response mechanisms.
- **Wildfires in Greece (2021):** The fires devastated vast areas of the country, destroying homes and infrastructure while putting many lives at risk. This crisis highlighted the need to review land management and update emergency plans.
- **Cyber-attack on the Irish healthcare system (2021):** This attack paralyzed healthcare services, demonstrating how cyber threats can have direct physical consequences and highlighting the need for strengthened cybersecurity measures.
- **Storm Alex (2020):** It affected Italy and France, highlighting the need for more resilient infrastructures capable of withstanding extreme weather events and underscoring the importance of cross-border cooperation.
- **COVID-19 pandemic (2020):** This global crisis highlighted the crucial importance of resilience for essential service operators. Various sectors such as healthcare, transportation, energy, telecommunications, food supply, etc., faced unprecedented challenges in maintaining operational continuity. The need to ensure worker safety and service continuity led to a rethinking of emergency management strategies and critical infrastructures resilience.

The COVID-19 pandemic has significantly accelerated the process of rethinking, redesigning, and enhancing resilience, pushing governments, companies, and individuals to recognize the importance of being prepared, adaptable, and collaborative in the face of global crises.

The relationship between resilience and pandemic contexts is the main focus of the Horizon Europe SUNRISE[44] project, which has explored the concept of resilience in terms of global strategy and specific pandemic-related issues, such as safety and protection of workers, rescheduling of activities to deliver services, cybersecurity in an abnormal context of IT service usage, and the use of new technologies to modify production process. ENDURANCE will benefit from the experiences, know-how, and results of SUNRISE and will establish ongoing collaboration through joint working groups.

To enrich and integrate lessons learned from past crisis experiences and from studies, research, and experiments conducted in European projects, additional inputs were gathered during the workshops organized in ENDURANCE, particularly the 4 local workshops in the pilot countries (Slovenia, Romania, Italy, and Greece) and the European workshop open to all interested parties. During these events, with a learning from CI approach, resilience stakeholders, operators, and authorities of essential services provided valuable contributions to the knowledge base on resilience, for which details can be found in the individual reports in section 4 (see the reference).

[43] Final report on the power system separation of Iberia from Continental Europe on 24 July 2021, https://www.entsoe.eu/news/2022/03/28/final-report-on-the-power-system-separation-of-iberia-from-continental-europe-on-24-july-2021/?utm_source=chatgpt.com.
[44] https://sunrise-europe.eu/

Key takeaways from lessons learned

From this initial analysis of the past events and available knowledge, the key lessons learned are as follows:

- **Cooperation:** Past events have highlighted the importance of improving cross-sector and, in some cases, cross-country cooperation. During emergency crises, individual operators' contingency plans are not sufficient. Enhanced knowledge of sectoral interdependencies is necessary through joint planning, which should not only be theoretical but also be accepted and implemented by the ecosystem through exercises and simulations.
- **Coordination:** Rapid and effective response in emergency situations cannot be achieved without adequate coordination of interventions. Experience has shown that fragmented interventions are ineffective in managing large-scale crises, leading to negative consequences for the communities and wasted resources.
- **Personnel Training and Crisis Readiness:** Analysis has revealed the necessity of improving personnel training in emergency management to ensure safety and protection, operational readiness, technical competence, effective communication, regulatory compliance, continuous improvement, and adaptation to emerging risk scenarios.
- **Prioritization:** Slow or ineffective responses to emergency crises have highlighted the need to define priority lists for services, users and locations. Additionally, the prioritization methodologies must consider the interconnections between essential service operators and move away from the siloed approaches.
- **Gap between prediction and reality** is still relevant. A significant gap remains between what can be predicted regarding threat impacts and what actually occurs when threats materialize. Theoretical models often fail in real scenarios. Advanced technologies must be adopted to develop realistic actionable solutions that reflect real-world challenges and stress-test existing systems.
- **Role of innovative technologies**: The adoption of new technologies and innovative solutions is vital for strengthening resilience. Technology-driven solutions must become integral infrastructure assets alongside other resources for day-to-day management. In some cases, the adoption of innovative technologies may face obstacles, including limited digitalization of systems and insufficient skilled personnel to implement the new technologies.
- **Role of cybersecurity:** Increasing digitalization of systems providing essential services creates growing exposure to cyber threats. All essential service operators must implement adequate cybersecurity systems, not only to ensure service provision but also to protect community safety and health Obsolete technologies and inadequate personnel skills remain obstacles to effective cybersecurity implementation.
- **Role of Government:**
    - Revise the land management to face destructive natural events.
    - Define a legal framework that supports resilience with a top-down approach.
    - Invest in and facilitate investments dedicated to resilience.
    - Improve communication with operators, ensuring clear communication that considers the diversity of individual operators (by sector and geographical context).

- **Unknown threats:** It is an atypical lesson learned, since there is no experience. However, considering ongoing global transformations, including the rapid spread of AI, escalating geopolitical and commercial crises, there is growing concern of emerging threats that remain poorly understood.

2.4 Analysis of EU Critical Infrastructure Protection (CIP) projects and initiatives related to resilience of critical entities and Essential Service Providers (ESP)

The European Union is actively enhancing the resilience of critical infrastructure in response to evolving cyber-physical threats, systemic vulnerabilities, and recent stressors such as pandemics, hybrid attacks, and extreme weather events. The **CER Directive (2022/2557)** and **NIS2 Directive** form the regulatory foundation, but the successful implementation of these directives depends on strategic innovation and cross-sector cooperation. EU-funded research and innovation projects are essential for this transformation, offering practical tools, strategies, and knowledge transfer mechanisms to critical sectors and entities.

In addition to its own research, ENDURANCE will benefit from the know-how and results of other European projects, that have addressed resilience with different focuses and perspectives, such as:

- ATLANTIS[45] focuses on resilience at the systemic level against combined cyber-physical threats and hazards, aiming to guarantee operational continuity while minimizing cascading effects.
- SUNRISE[46] focuses on strategies and technologies for united and resilient critical infrastructure and vital services in pandemic-stricken Europe. These are a key finding for resilience in a case of pandemic situations.
- PRECINT[47] focuses on physical and cybersecurity threat management and cascading effects in defined geographical areas.
- InfraStress[48]addresses cyber-physical threats to Sensitive Industrial Plants and Sites where different types and sectors of critical infrastructure operators are interconnected.
- CyberSEAS[49] focuses on cybersecurity in European Power and Energy Systems (EPES)
- APPRAISE[50] focuses on big data analysis and artificial intelligence, enabling the creation of robust security frameworks to improve both the cyber and physical security and safety of public spaces.

Key EU Projects Enhancing CI and ESP Resilience

This section examines key highlights of individual EU projects that significantly impact the development of understanding critical infrastructure resilience.

[45] https://www.atlantis-horizon.eu/
[46] https://sunrise-europe.eu/
[47] https://www.precinct.info/en/
[48] https://cordis.europa.eu/project/id/833088
[49] https://cyberseas.eu/
[50] https://www.appraise-h2020.eu/

A. EU-CIP (2022-2025)

- **Full Title:** European Knowledge Hub and Policy testbed for Critical Infrastructure Protection
- **Focus**: Security and resilience of infrastructure and services essential to society. The main goal of EU-CIP is to establish a novel pan-European knowledge network for Resilient Infrastructures, enabling policy makers to develop data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs).
- **Key Outputs**: Risk assessment methodologies, cross-border cooperation strategies, public-private partnership frameworks, sectorial white papers and a domain library for CIP.
- **Relevance**: The project provides strategic and operational mechanisms for multi-sectoral collaboration across the EU, enhancing situational awareness and coordinated responses.

B. ENDURANCE Project (2024–2027)

Full Title: Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe

- **Objective**: Develop a unified strategy for improving the resilience of critical entities across Member States.
- **Activities**: Stakeholder engagement, gap analysis, development of use cases, and recommendations for policy harmonization.
- **Contribution**: The project offers practical tools and procedures for CER Directive implementation and supports harmonized resilience-building across sectors.

C. ATLANTIS (2022-2025)

- **Full Title:** Enhancing Resilience and Systemic Cyber-Physical-Human Security of EU Critical Infrastructures
- **Focus:** The project aims to improve systemic resilience across EU Critical Infrastructures (CI) by considering **Cyber-Physical-Human (CPH)** security. It develops integrated tools and decision-support systems that assess risks and coordinate responses across complex infrastructure ecosystems. Uses innovative technologies like **digital twins**, **sensor fusion**, and **AI-enhanced situational awareness**. Promotes collaboration between CI operators, public authorities, and security experts to address cascading and coordinated threats.

D. SUNRISE (2022-2025)

- **Full Title:** Strategies and Technologies for United and Resilient Critical Infrastructure and Vital Services in Pandemic-Stricken Europe
- **Focus:** Developed in response to the urgent need to enhance CI and ESP resilience during and after pandemics (e.g., COVID-19). Delivers **risk governance frameworks**, **interoperable tools**, and **cross-sectoral collaboration protocols**. Helps ESPs (health, transport, water, energy) identify vulnerabilities, optimize business continuity planning, and adapt operations to extreme disruptions. Strong emphasis on **preparedness, continuity of vital services**, and **strategic foresight** for systemic shocks.

E. PRECINCT (2019-2021)

- **Full Title:** Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-physical Threats and Effects

- **Focus:** The project tackles complex cyber-physical threats across interdependent infrastructure systems, especially at **district and regional levels**. It combines **digital twin technology** with a **Community Platform** to support collaborative risk analysis and coordinated response. Aims to protect against cascading effects of cyber-physical incidents, including natural hazards, cyberattacks, and insider threats. Enables public-private partnerships to improve resilience planning and real-time risk management.

F. EFAS (European Flood Awareness System) and Copernicus Emergency Services[51]

- **Focus**: Provide early warnings and situational awareness for natural disasters. The European Flood Awareness System (EFAS) is part of the Copernicus Emergency Management Service (Copernicus EMS). It provides complementary, flood early warning information to its partners, the National/Regional Hydrological Services and the European Response and Coordination Centre (ERCC). EFAS holds a large-variety of regularly updated flood forecast information ranging from gridded hydro-meteorological variables, modelled soil moisture, runoff and snow data, to a wide-range of flood-related information such as probabilistic medium-range flood forecasts (including short-range flash floods), seasonal forecasts, impact assessments and early warnings. Real-time forecast information is available to EFAS partners only. Archived EFAS information is publicly available. Real-time data and services are accessible to EFAS partners only on the EFAS web interface and can be downloaded via an SOS and WMS-T service and from a data archive (foreseen development). Archived data is available publicly.
- **Application**: Supports critical infrastructure operators and ESPs in risk mitigation and preparedness.

G. EU RESILIENCE DASHBOARDS

Focus: The resilience dashboards provide a holistic assessment of the ability to progress amidst ongoing societal transformations and challenges ahead, across four dimensions:

  - social and economic
  - green (environmental)
  - digital
  - geopolitical

They have been developed by the European Commission in a process of collective intelligence with Member States and other relevant stakeholders, as a follow up to the 2020 Strategic Foresight Report.[52]

They represent a forward-looking monitoring tool for the transition-led EU policy agenda and aim to help Member States identify areas for further analysis and potential policy actions.

The resilience dashboards aim to provide a holistic assessment of resilience in the EU and its Member States. In relation to ongoing societal transformations and challenges ahead, the dashboards assess resilience as the ability to make progress towards policy objectives amidst challenges.

Through a broad set of indicators, the resilience dashboards assess the relative strengths and weaknesses of countries. They also help Member States to identify areas for further analysis and

[51] European Flood Awareness System, Acronym: CEMS-EFAS, https://data.jrc.ec.europa.eu/collection/id-0068.
[52]2020 Strategic Foresight Report, https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en.

potential policy actions. The indicators span four dimensions: social and economic, green, digital, and geopolitical.

For a subset of indicators, they also show how the EU-27 is doing with respect to selected countries outside the EU.

The dashboards include a selection of indicators that show:

- Capacities - enablers and/or opportunities to navigate the transitions and face future shocks;
- Vulnerabilities - obstacles or aspects that can worsen the negative impact of the challenges related to the green, digital, and fair transitions.

The selection of these indicators was made with a forward-looking perspective, informed by strategic foresight. The indicators are strongly linked to relevant megatrends – long-term driving forces that will most likely have significant impacts on Europe's future.

The detailed dashboards for both EU and non-EU countries are complemented by synthetic resilience indices. These indices aim to illustrate the overall relative resilience capacities and vulnerabilities across the four dimensions.

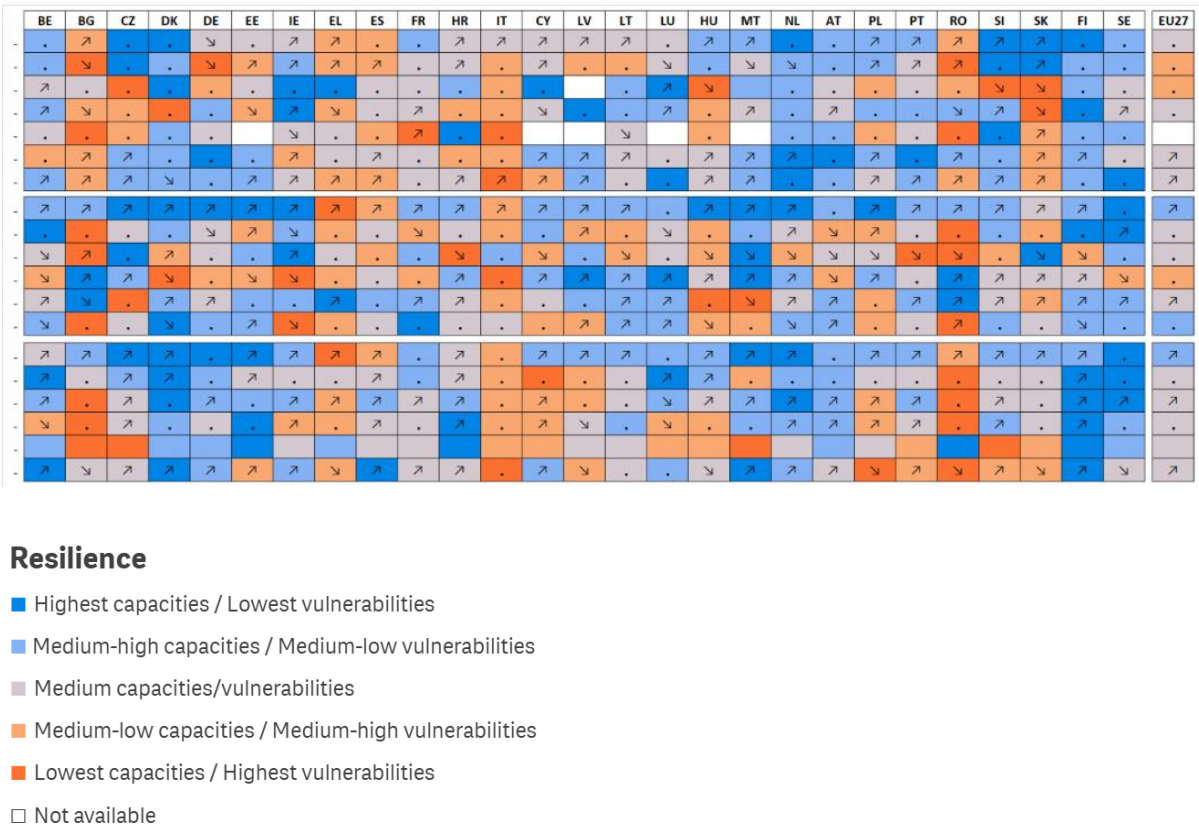


Figure 2: Resilience per EU countries.

H. THE EUROPEAN CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES (ECSCI):

ECSCI plays a pivotal role in enhancing the resilience and security of Critical Infrastructures (CI) across the European Union. ECSCI is a strategic initiative that brings together a range of EU-funded projects, industry partners, research institutions, and policy stakeholders, aiming to foster collaboration, knowledge sharing, and synergies across various domains of critical infrastructure protection (CIP).

Key Roles:

- **Facilitating Cross-Project Collaboration**

ECSCI serves as a central platform where ongoing EU projects focused on critical infrastructure security can exchange results, align objectives, and coordinate efforts. This collaboration reduces duplication of research, encourages harmonized methodologies, and allows projects to build upon each other's findings.

- **Integrating Multi-Sectoral and Multi-Hazard Approaches**

ECSCI promotes a holistic view of resilience, addressing both physical and cyber threats as well as natural and man-made hazards. By doing so, it enhances systemic understanding and strengthens protection strategies across sectors like energy, water, transport, healthcare, and digital services.

- **Supporting Policy and Standardization Efforts**

The cluster provides valuable insights and evidence to support EU policy-making and the implementation of directives such as the CER Directive and the NIS2 Directive. ECSCI's outcomes also contribute to the development of technical standards and frameworks that underpin security and resilience best practices across member states.

- **Enhancing Innovation and Technology Transfer**

By linking research with real-world applications, ECSCI encourages the uptake of innovative technologies and tools developed through EU projects. It supports demonstrations, pilot implementations, and the creation of interoperable solutions that can be adopted by critical infrastructure operators and competent authorities.

- **Dissemination and Stakeholder Engagement**

ECSCI acts as a hub for communication and dissemination, ensuring that knowledge reaches a wide range of stakeholders—including policymakers, infrastructure operators, emergency responders, and the academic community. Regular events, publications, and workshops foster engagement and capacity building.

- **Strategic Foresight and Road mapping**

The cluster helps define long-term research and innovation priorities by identifying emerging threats, gaps in current capabilities, and future needs. It contributes to roadmaps and strategic planning that guide the evolution of CIP research at the European level.

ECSCI significantly contributes to the resilience, preparedness, and adaptive capacity of critical infrastructures in Europe. It not only bridges the gap between research and implementation but also

fosters a unified, proactive, and forward-looking community committed to safeguarding essential services against evolving threats and challenges.

Insights and Impact

The dynamic landscape of critical infrastructure protection requires not only innovative solutions but also a deep understanding of the practical implications of research and development efforts. The "Insights and Impact" section captures key findings, lessons learned, and the broader influence of ongoing initiatives on policy, practice, and operational resilience. These insights reflect both strategic advancements and tangible benefits delivered through collaboration, technological innovation, and stakeholder engagement across Europe.

- **Multi-Level Risk Governance**: Projects address resilience from strategic (policy), operational (response tools), and tactical (real-time monitoring) angles.
- **Digital Transformation for CI Resilience**: All three projects leverage digital twins, AI, and data-driven modelling to simulate disruptions and optimize interventions.
- **Cross-Sectoral Collaboration**: Key emphasis on cooperation between sectors (e.g., health, transport, energy) and between private/public actors.
- **Cascading Risk Management**: ATLANTIS and PRECINCT, in particular, prioritize understanding and mitigating the domino effects of complex threats.
- **Post-Pandemic Readiness**: SUNRISE is a cornerstone for preparing for future systemic disruptions, aligning health and infrastructure resilience planning.

Key Findings

The section summarizes the most critical observations and conclusions drawn from research activities, stakeholder engagement, and project implementation. These findings offer a clear overview of the current state of resilience across critical entities and essential service providers, highlighting systemic gaps, emerging trends, and successful approaches. They serve as a foundation for shaping future strategies, improving policy alignment, and guiding practical interventions to enhance the robustness and responsiveness of Europe's critical infrastructure systems.

A. Shift from Protection to Resilience

Projects increasingly emphasize continuity, adaptability, and systemic resilience over static protection. This aligns with EU's CER Directive and resilience-building for ESPs.

B. Cross-Sector and Cross-Border Collaboration

Many initiatives, such as EU-CIP and ENDURANCE, prioritize multi-sectoral engagement, which is critical for interdependent systems like energy, transport, water, and digital infrastructure.

C. Gaps and Challenges Identified

- Limited integration of small and medium-sized ESPs.
- Lack of consistent application of resilience metrics.
- Uneven maturity levels across Member States regarding CER and NIS2 implementation.

- Limited sharing of threat intelligence and lessons learned across sectors.

D. Best Practices Observed

- Regular stress testing and scenario planning.
- Engagement of ESPs in co-development of resilience solutions.
- Use of digital twins and AI for predictive resilience modelling.
- Incorporation of climate adaptation into CIP strategies.

Strategic Recommendations

The Strategic Recommendations outlined in this section are derived from comprehensive analysis, stakeholder feedback, and lessons learned from EU-funded projects and initiatives. They aim to support policymakers, critical infrastructure operators, and other key stakeholders in strengthening the resilience and security of essential services across Europe. These recommendations focus on promoting systemic collaboration, enhancing regulatory alignment, fostering technological innovation, and ensuring sustained investment in risk management and preparedness capabilities.

- **Integrate Outcomes into National CER Implementation Plans**
  Use tested tools, guidelines, and platforms from these projects to inform national and local CI resilience frameworks.
- **Promote Interoperability Across Critical Sectors**
  Align data sharing protocols, risk classification, and digital infrastructures as modelled by ATLANTIS and PRECINCT.
- **Empower Local and Regional Authorities**
  Extend project results to regional and municipal CI operators through dedicated pilot programs and resilience labs.
- **Foster Community Participation and Skills Development**
  Use community platforms like in PRECINCT to promote end-user engagement and collaborative scenario planning.
- **Sustain and Scale Best Practices**
  Ensure that the insights, technologies, and methodologies developed are maintained, updated, and accessible post-project through EU-level platforms or Centers of Excellence.

Projects are critical building blocks of Europe's strategy to secure and future-proof essential services and infrastructure. They reflect a shift from reactive to proactive resilience—one that is digitally enabled, user-centric, and policy-aligned. Leveraging these innovations at the national, regional, and local levels will be key to creating a resilient, secure, and sustainable European infrastructure landscape.

3 Use cases

Analysis of Representative Use Cases Most Applicable for Societal Resilience provides an in-depth examination of selected use cases that exemplify challenges and solutions in ensuring the resilience of societies across sectors. The aim is to explore real-world scenarios that illustrate the multifaceted nature of threats ranging from cyber and hybrid attacks to natural disasters and supply chain disruptions and how different critical entities respond and adapt. These representative cases offer valuable insights into vulnerabilities, best practices, and the importance of coordinated action among public and private stakeholders. By drawing lessons from actual disruptions and tested mitigation strategies, this analysis supports the development of actionable models for enhancing the robustness, adaptability, and recovery capacities of essential services at national and EU levels.

Building upon the analysis above, this section Indication of Use Cases for Pilots in ENDURANCE proposes a set of use cases that are particularly suited for piloting within the ENDURANCE project framework. The selected pilot cases are chosen based on their relevance to cross-border cooperation, sectoral interdependencies, and applicability across diverse critical infrastructure domains (e.g., energy, health, transport, digital services). Each use case serves as a testing ground for validating the effectiveness of proposed strategies, technologies, and collaborative mechanisms aimed at improving situational awareness, risk management, and rapid response. These pilots will enable iterative learning, stakeholder engagement, and real-time evaluation, contributing to the refinement of the ENDURANCE resilience framework and tools.

3.1 Analysis of representatives use cases most applicable for resilience of societies

In order to address resilience with a holistic approach and its variations based on the sector, geographic area, and the specificity and variability of the threats to which operators and authorities of essential services are exposed, a template (ANNEX:1) has been prepared for the collection of data and information regarding individual organizations (operators and authorities) and their positioning towards the various threats they are exposed to, capable of identifying potential vulnerabilities and improvement areas to ensure better resilience.

ENDURANCE partners provided data and information enabling the profiling of their organization in relation to all possible risk scenarios and related impacts. Given that some data and information collected from critical infrastructures, could highlight some vulnerabilities of the organizations and sensitive information, we analyzed and elaborated the received input in order to provide an overview of the main relevant risk scenarios belonging to the following categories of ENDURANCE all-hazard approach:

- Cyberattacks
- Natural disasters
- Human errors
- Environmental issues

- Health emergencies

For each category, specific threats have been defined according to the type of organization, broadly highlighting both internal and external impacts on the organization itself, as outlined below.

CYBERSECURITY

Energy (Operator)

1 Threat: Generic cyber-attack

Internal impact: Most critical and vulnerable subsystems are operational and control systems.

External impact: all sector and citizens.

Telecommunication (Operator)

2 Threat: cyber-attack on the information resources necessary for the operation of the internal network

Internal Impact: LAN outage, company's business processes are affected

External impact: Potential cascading effects on energy supply, government, transportation, and emergency response coordination. By default, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

3 Threat: Cyber DDos attack

Internal impact: The IT security department, network administration, and customer service platforms would be impacted.

External impact: Potential cascading effects on energy supply, government, transportation, and emergency response coordination.

4 Threat: Cyber Ransomware Infection, that can be caused by different ways such as:

- infection with a ransomware virus via e-mail (infected attachment, link to an infected file, use of social engineering methods, etc.),
- infection with malicious code when installing applications from unauthorized or unknown sources,
- launching applications and other software that has not been previously approved, and security checked,
- introduction of malicious code via user equipment that connects to the company's business network (mobile phones, USB sticks and other information sources),
- infection and automated distribution of malicious code via vulnerable information assets,
- infection via infected software in the supply chain (there are known cases when even established companies unknowingly had parts of malicious code in their software that they received from (sub)suppliers),
- activation of a ransomware virus on company workstations, etc.

Internal impact; IT security department, network administration, and customer service platforms would be impacted.

External impact: Potential cascading effects on energy supply, government, transportation, and emergency response coordination.

Telecommunication (digital services provider)

5 Threat: Ransomware attacks on critical infrastructure

Internal impact: Cyberattack—ransomware propagating through interconnected systems, leading to encrypted files, system lockouts, and potential extortion. The most impact can be on: IT Infrastructure (servers, storage, cloud systems), Operational Technology (OT) controlling critical services, Identity and Access Management (IAM) systems, The most vulnerable are endpoints, unpatched software, and shared network storage.

External impact: the cascading effects are on Customer support (unable to assist clients), Finance (payment disruptions), IT (system restoration, security response), Operations (halted services), Disrupted communications (telecommunication sector), Potential power outages if SCADA systems are hit (Energy), Delayed emergency services (healthcare sector), Cloud services hosting critical applications (Digital Infrastructure sector) (Cloud services hosting critical applications).

6 Threat: Exploiting software vulnerabilities

Internal impact: on the company's digital infrastructure and related services such as customer support on all levels, sales, SW Development, human resources and finance.

External impact: on Telco, Energy, Public Safety, in case of SLA breach.

Telecommunication (Local Authority)

7 Threat: cyber-attack - compromised data

Internal impact: outage of internet service and potential data breach affects:

- Technical subsystems – IT infrastructure, servers, networks, databases, applications, security systems, etc.
- Organizational subsystems – various departments or business units with specific tasks (IT support, legal department, human resources…).
- Operational subsystems – processes and mechanisms that ensure the smooth functioning of the organization.
- Externally connected subsystems – cooperating partners, suppliers, and services essential for business operations (e.g., internet service providers, electricity distribution, logistics services).

External impact: Operators or clients that communicate by electronic networks.

Telecommunication (National Authority)

8 Threat: cyberattack focusing on interception of information, malicious code/ software/ activity or identity theft.

Internal impact: communication system.

External impact: all sectors of critical infrastructure.

Government for security (National Authority)

9 Threat: Cyber ransomware attack on the IT&C infrastructure at national level

Internal impact: a cyber ransomware attack targets the web mail server used by employees of the central structure of the MAI, the attack does not compromise classified data but could expose sensitive or non-public information. The ransomware attack on the web mail server disrupts internal communication by preventing employees from accessing emails, delaying coordination, decision-making and essential administrative processes. Additionally, the breach risks the exposure of sensitive but non-classified information, including personal data, internal discussions, security briefings, investigative details and operational procedures. Even if the data is not officially classified, its leakage could compromise security strategies, reveal personnel details and pose reputational risks.

External impact: The public administration and national security sector will be the most impacted, as the ransomware attack on the web mail server disrupts law enforcement, crisis management and internal coordination. Law enforcement and security agencies will face delays in investigations, intelligence sharing and emergency responses, potentially increasing security risks. The public will also be affected, experiencing service disruptions, delays in administrative processes and potential exposure of sensitive personal data, leading to privacy concerns and reduced trust in authorities.

Cybersecurity Agency (National Authority)

10 Threat: Advanced Persistent Threat (APT)

Internal impact: the Identity & Access Management (IAM) System, Classified & Secure communications System are the main effect sub-area.

External impact: a successful APT attack would have significant cascading effects across multiple critical sectors. An adversary gaining access to our threat intelligence or incident response platforms could compromise our ability to detect and respond to attacks against energy infrastructure, financial services, healthcare systems, and government services. The highest risk sectors include energy (electrical grid operators), healthcare (hospital networks), financial institutions (banking systems), and critical government operations that rely on the Authority for cyber threat monitoring and incident coordination.

11 Threat: Cyber Incident response and coordination

Internal impact: Multiple critical subsystems including National CSIRT infrastructure, National Cyber Crisis Management Center, monitoring and detection systems, communications networks, incident

reporting platforms, and certification systems. Most critical: National Platform for Reporting Cyber Security Incidents (PNRISC) and CSIRT infrastructure.

External impact: All sectors relying on digital infrastructure would be impacted, particularly critical infrastructure operators, essential service providers, public administration, and healthcare. Moreover, a compromised ability to coordinate incident response would have cascading effects across multiple sectors, including public administration, healthcare, energy, transportation, and financial services.

Digital Operator + Regional Government (Regional Authority)

12 Threat: Citizen's data exfiltration and information technology infrastructure compromission through Supply Chain attack with VPN credential stuffing

Internal impact: Application Server / Software Application / Databases / Dependencies to external web services / Reverse Proxy / Gateway / DMZ / Identity Service Management. The most critical subsystem in this scenario are Databases, Server and Identity Management Service; other are the Domain Controller and the Active Directory of the vendor and belonging to the Public Administration.

External impact: delay or interruption of all online public services provided to citizens and enterprises. All digital communication with other public entity at local and national.

13 Threat: Cyberattack against specifics applications and services that manage the election processes

Internal impact: data fabrication and disruption inside the application database.

External impact: make invalid the result of election process.

14 Threat: Human sabotage of Datacenter's Safety systems

Internal impact: People with malicious intent damage the safety system of the Datacenter's building in order to create harm to people and assets. The most critical subsystem are the assets inside the Datacenter that manage the publication of different services to Publica Administration and Health Sector.

External impact: Health sector and publica administrations that use digital public services.

15 Threat: Citizen's data exfiltration and regional information technology infrastructure compromission through insider threats attack. The source can be Spear phishing / Evil Twin / Infostealer / initial compromission of a vendor belonging to the supply chain

Internal impact: Application Server / Software Application / Databases / Dependencies to external web services / Reverse Proxy / Gateway / DMZ / Identity Service Management. The most critical subsystem in our scenario are Databases, Server and Identity Management Service; other are the Domain Controller and the Active Directory of the vendor and belonging to the local context.

External impact: delay or interruption of all online public services provided to citizens and enterprises. All digital communication with other public entity at local and national.

Healthcare (Hospital)

16 Threat: Exploiting software vulnerabilities

Internal impact: functioning of digital infrastructure and medical supply chain.

External impact: public safety and medical treatment.

Water (Local Operator)

17 Threat**:** Synchronized attack on water treatment facilities

Internal impact: Two main subsystems. Drinking water subnetwork and Wastewater subnetwork. Both networks are accompanied by their main operational units (water treatment units and wastewater treatment plants). Both subsystems are equally critical, each one having its own dependencies and consequences. One of the main risk scenarios is a cyber-attack to create panic and distraction, such as create false alter to the operator in order to cause distraction of the personnel and to proceed with a water contamination action of a not-surveilled area.

External impact: if the attack persists for an extended amount of time, it threatens to the health and well-being of residents in the affected area.

18 Threat: Terrorist attack on water cleaning facilities

Internal impact: A potential hacker is connected to the management system targeting to affect the smooth operation of the facility by interfering with an installed CBRN. This causes panic among the personnel and major chemicals could be released into water (more that needed amount). The two main system are exposed to this risk.

External impact: Public safety and drinking water for citizens and other sectors in the affected area.

NATURAL DISASTERS

Energy (National Operator)

1 Threat: all extreme natural events, such as flooding, storms, cold spell, forest fire, earthquake

Internal impact: subsystems for transmission of electrical energy., such as Transmission Network Infrastructure Unit / System operations Unit / Corporate security Unit. Operational damage to the equipment. It may also be harmful to the people.

External impact: Energy sector and specific business sector and consumers on the area where natural disaster happens. It means potentially cross-sector impact, like transport, health, digital.

Telecommunication (Operator)

2 Threat: prolonged heatwave during summer season

Internal impact: Stable operation of server systems is crucial for ICT companies. In summer season cooling prevents overheating, which can cause failures. A large-scale power outage can lead to the failure of cooling systems, which seriously threatens the infrastructure. Without cooling, the temperature in server rooms rises quickly, causing servers to shut down, loss of connectivity and application downtime. Although data centers have protection mechanisms such as redundant fans and passive cooling, these measures are only effective for a limited time

External impact: By default, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

3 Threat: Sleet, snow

Internal impact: A longer period with heavy accumulation of snow could impact on access to the sites of the infrastructure. The most critical and vulnerable subsystems are: base stations, power-dependent network elements mainly on the field and fiber optic cables. Multiple business units, including network operations, field maintenance, and customer support, would be affected.

External impact: By default, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

4 Threat: Floods:

Internal impact: floods that can cover areas where infrastructure is located on the ground with water, also in connection with landslides, the removal of a certain part of the land. The most critical and vulnerable subsystems are: network access points, base stations, and underground fiber optic cables with an impact on multiple business units, including network operations, field maintenance, and customer support.

External impact: Potential cascading effects on energy supply, government, transportation, and emergency response coordination, due to interdependencies with telco communication services, such as phone, SMS, internet, or cloud.

5 Threat: sever earthquake

Internal impact: a strong earthquake can affect several company buildings, completely destroyed or partially damaged, including equipment and information resources located in these buildings. Some premises or facilities are unusable for a long time (weeks or even months) for carrying out business processes, and practically all key services are affected. Moreover, servers, equipment, network access points, base stations, and underground fibre optic cables can be affected by earthquake.

External impact: Potential cascading effects on energy supply, transportation, and emergency response coordination. In general, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

Authority for Cybersecurity (National level)

6 Threat: sever earthquake

Internal impact: Seismic event (earthquake) that could damage physical infrastructure, disrupt power and connectivity, and render key facilities inoperable. Secondary concerns include structural damage to data centers, cooling system failures, and staff unavailability. Most vulnerable are on-premises data centers, primary power systems, and cooling infrastructure that rely on physical facilities.

External impact: The inability to monitor and respond to cyber threats during a natural disaster creates a compound risk where adversaries could exploit the situation. Critical sectors affected include healthcare (hospital systems), energy infrastructure, telecommunications, emergency response systems, and transportation management systems.

Health (Hospital)

7 Threat: sever earthquake

Internal impact: Seismic event (earthquake) that could damage physical infrastructure, disrupt power and connectivity, and render key facilities inoperable.

External impact: Medical supply chain, Public Health and Safety

Digital Operator + Regional Government (Regional Authority)

8 Threat: sever earthquake

Internal impact: on critical systems: ICT infrastructures, data centers, essential public services, offices and operational centers vulnerable to natural disasters. Failure of

- Healthcare facilities (hospitals, nursing homes, outpatient clinics)
- Critical infrastructure (telecommunications, energy, transportation networks)
- Emergency services (Civil Protection, Fire Brigade, law enforcement)
- Public sector (municipalities, prefectures, territorial management entities

External impact: chain reactions in:

- The energy distribution network, leading to potential blackouts
- The water supply network, affecting access to drinking water
- Mobility, with damage to roads, bridges, and railways
- Communications, hindering emergency operations coordination

Water (Local Operator)

9 Threat: Prolonged Drought

Internal impact: The two main subsystems, drinking water subnetwork and wastewater subnetwork, can be affected. Both subsystems are equally critical, each one having its own dependencies and consequences.

External impact: Residents and all sectors of the interested area are affected by this natural disaster. Operators will need to find alternatives water resources to feed the water to fill the water pipes and to convince consumers to reduce water consumption to the absolute minimum, especially during the summer months.

10 Threat: Flood

Internal impact: Severe Storms with Heavy rains cause flooding, in some areas, causing stormwater drains to overflow and a large portion of the water end up in the water supply and sewerage networks. Drinking water subnetwork and Wastewater subnetwork are accompanied by their main operational units (water treatment units and wastewater treatment plants). Both subsystems are equally critical, each one having its own dependencies and consequences.

External impact: Residents of areas affected by the outage. Operator who will need to provide resources (people/machinery) to recover the issue in parallel with possible customer loss and cost loss. In addition, traffic on the roads is affected. If the overflow persists for an extended amount of time, threats to the health and well-being of residents in the affected area. Apart from that, depending on the magnitude of the damage and the length of repairs traffic towards the impacted area can be disrupted, affecting transportation and socioeconomical life.

11 Threat: The appearance of turbidity in a clean water reservoir

Internal impact: All water reservoirs can be potentially involved. All are critical since they provide drinking water to the population.

External impact: The consumers supplied by the reservoir have been put at risk. Different reservoirs supply different consumers depending on their geographical location. In addition to the individuals whose supply of clean water will be affected, businesses whose operations are critically dependent on water supply.

Water (Local Authority)

12 Threat: Flood disrupting agriculture activities & transportation

Internal impact: damage of infrastructure, problems on a lot of different subsystems, Civil protection, technical unit, agricultural unit, (waste) water management services.

External impact: Farmers are the most impacted category. Economic hardship caused by crop loss can create social disruption and have cascading effects on the food sector. Transport sector may be also affected.

TECHNOLOGICAL HAZARD

Energy (National Operator)

1 Threat: **Equipment failure**

Internal impact: on infrastructure for transmission of electrical energy, such as Transmission Network Infrastructure Unit / System operations Unit / Corporate security Unit.

External impact: Potentially it can involve other stakeholders in the energy sector and all other sectors that depend on electricity on specific area.

Telecommunication (Operator)

2 Threat: technical failure of hardware or software

Internal Impact: LAN outage, company's business processes are affected.

External impact: Potential cascading effects on energy supply, government, transportation, and emergency response coordination. By default, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

3 Threat: Accident Near the Company Building

Internal impact: the company's facilities and the equipment in them and the people are usually not damaged, but due to the extent of the accident, further use of this facility is temporarily impossible due to the failure of supply services (power, heating, etc.), the inaccessibility of the facility (damaged or destroyed access routes), or the approach and use of the facility are dangerous (e.g. leakage of toxic substances, risk of explosion, etc.). The consequences of this emergency depend on the type of facility affected. In some cases, all business processes that are carried out at the location of the affected facility are affected. Since most key technological solutions operate in a duplicated setup at different locations, the operation of such key company services is less affected, while individual business processes carried out by employees in these facilities may be more affected.

External impact: On users requiring uninterrupted digital services. Low probability of cross sector impact.

4 Threat: Fire on site

Internal impact: A fire broke out at a company location. Due to the fire or its extinguishing, the equipment in the premises, including the information resources that were there, was partially or completely damaged and destroyed. As a result, the premises or facility are unusable for business processes for a long time (weeks or even months). Due to the fire or its extinguishing, the equipment in the premises, including the information resources that were there, was partially or completely damaged and destroyed.

External impact: Users requiring uninterrupted digital services. Potential cascading effects on energy supply, transportation, and emergency response coordination. In general, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

Water (Local operator)

5 Threat: Disruption to drinking water supply caused by infrastructure failures

Internal impact: due to aging infrastructure, this is the largest risk for water operator. The immediate impact is unavailability of the service and possible flooding around water and wastewater disruption Two main subsystems affected are drinking water subnetwork and wastewater subnetwork. Both networks are accompanied by their main operational units (water treatment units and wastewater treatment plants). Operator will need resources (people/machinery) to recover the issue in parallel with possible customer loss and cost loss.

External impact: Residents of areas affected by the outage. Low trust from citizens' side.

ENVIRONMENTAL

Telecommunication (National Operator)

1: Threat: Electromagnetic pulse (EMP)

Geomagnetic storms are caused by powerful solar eruptions, such as coronal mass ejections (CMEs) or solar flares, which send large amounts of charged particles (plasma clouds, which is a powerful burst of electromagnetic energy) into the Earth's magnetosphere. These particles cause disturbances in the Earth's magnetic field, which can seriously affect various parts of the infrastructure, especially telecommunications systems. An electromagnetic pulse (EMP) is a sudden and powerful burst of electromagnetic energy that can cause disruption or even permanent damage to electronic devices and infrastructure. The causes can be:

- Geomagnetic storms – Powerful solar flares (coronal mass ejections – CMEs) can cause geomagnetic storms that induce electrical currents in power and telecommunications networks.
- High-Altitude Electromagnetic Pulse (HEMP) – A nuclear bomb explosion 30–400 km above Earth can cause a wide area of devastating EMP that could damage electrical and communications systems across an entire continent.
- Non-nuclear EMP weapons (NNEMP) – Specially designed devices, called EMP generators or micro-wave weapons, can emit powerful electromagnetic pulses to disable electronic systems without the use of nuclear weapons.
- Local plasma clouds – sometimes natural plasma clouds occur in the ionosphere, which can trigger localized electromagnetic pulses when they interact with the Earth's magnetic field.
- Possible plasma cloud coming from the interplanetary space.

Internal impact: The consequences of the event and possible impacts are as follows:

- The impact itself can be completely local in nature (as in the case of lightning).
- The impact can be much larger and such an EMP can affect and damage electronic devices thousands of kilometers away.
- Plasma in the ionosphere can act as a natural or artificial trigger for an electromagnetic pulse that can affect electronic systems and telecommunications.
- While geomagnetic storms create slower and longer-lasting disturbances, artificial explosions in the ionosphere can trigger powerful and immediate EMP effects that cause damage over large areas.
- These changes can cause geomagnetic induced currents (GICs) in the power grid and create low-frequency EMF effects that disrupt electronic devices.

- Electrostatics and electronics degradation: Prolonged exposure to geomagnetic storms can cause radiation damage to satellite electronics, which can lead to their failure or loss of control. This can be also true for the electronics on the ground (the Earth)
- Charged particles (from the Sun) can cause changes in the ionosphere, which can disrupt radio and satellite signal transmission.
- Power grid outages – if induced geomagnetic currents were to cause transformer failure in power systems, there could be long-term power outages worldwide.

External Impact: In general, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

2: Threat: GPS and NTP degradation

Internal impact: GPS signals can be degraded or completely disrupted by both geomagnetic storms and electromagnetic pulses (EMP) in different ways, described below:

- Since GPS satellites transmit signals at very low power (~50 watts or less), they are especially vulnerable to interference from an EMP.
- Since NTP servers mainly depends on GPS, NTP servers could be degraded as well. The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP uses a hierarchical, semi-layered system of time sources.
- Geomagnetic storms are caused by powerful solar eruptions, such as coronal mass ejections (CMEs) or solar flares, which send large amounts of charged particles (plasma clouds, which is a powerful burst of electromagnetic energy) into the Earth's magnetosphere. These particles cause disturbances in the Earth's magnetic field, which can seriously affect various parts of the infrastructure, especially telecommunications systems.

Internal impact: the entire spectrum of infrastructure, this applies to electronic infrastructure (like network, network access points, base stations, fiber optic cables). On the one hand, it can affect problems related to the power supply of electronic systems. In addition, EMF can also affect individual electronic devices, such as computers, servers, mobile phones, and other electronic devices depending on Hardening Techniques & Component-Level Protection against EMP.

The most critical and vulnerable subsystems based on the risk scenarios are:

- 5G and 4G Networks need precise time synchronization for data packet coordination. A loss of GPS time can cause dropped calls, slow data rates, and network failures.
- Time-sensitive database operations (e.g., logs, security audits, distributed computing) require precise synchronization. If timestamps drift, it can cause data corruption, security breaches, and loss of service.
- Many security protocols (e.g., Kerberos, TLS certificates) rely on accurate time. A drift in timestamps can cause authentication failures, session timeouts, and security vulnerabilities.

External impact: Potential cascading effects on energy supply, government, transportation, and emergency response coordination. By default, all sectors can be impacted, which relay on telco communication services, and which uses its services, that can be phone, SMS, internet, or cloud.

HEALTH EMERGENCY

CROSS-X (sector, country, organization)

Pandemic

Internal impact: human resources of all organization. Sick workers cannot work. All area of an entity can be affected. Possible interruption of services.

External impact: limited availability of services for all customers or users of essential services.

3.2 Indicative use cases for pilots in ENDURANCE

Following an activity aimed at identifying potential risk scenarios to which operators and authorities of essential services may be exposed, specific threats were selected as the basis for developing individual **micro pilots** in the sectors of **Public Administration** and **Water Management**, in Italy and Greece respectively, as well as **meso pilots** in the **Digital-Energy** and **Digital-Health** sectors, in **Slovenia** and **Romania** respectively.

These pilots provide a detailed view—both sector-specific and cross-sectoral—at the national level, which will be expanded to a European scale through the **Macro pilot**, with the aim of evaluating the overall **Strategy** and conducting a **Risk & Resilience Assessment**.

An input-output cycle between the micro/meso pilots and the macro pilot will serve as an **iterative and scalable process**, in which evidence, solutions, and critical issues identified at the local and sectoral levels will be systematically collected, analyzed, and transferred to support the enhancement of resilience of interconnected critical services across Europe, and vice versa.

The description of the micro and meso pilot use cases has been guided by a common template, applied across all pilots, in order to gain a comprehensive understanding of:

- How the threat may evolve within a specific sectoral or geographical context, and the types of damage it may cause to different actors;
- What the needs and expectations are in terms of reducing and mitigating the potential impacts of the threat;
- The **AS-IS** situation, describing the current flow (who, what, how, data);
- The **TO-BE** situation after the implementation of ENDURANCE, including interactions with existing processes, constraints and limitations, and missing or new data;

3.2.1 MESO PILOT – SLOVENIA

Organization	Slovenian pilot included two main CI operator for given sectors (Energy and Telecommunication) Telekom Slovenije (TS) and Slovenian Electro energy TSO (ELES) and two important national coordinators, National cybersecurity authority (Government Information Security Office - URSIV) and National regulatory authority in the field of electronic communications (Agency for Communication Networks and Services of the Republic of Slovenia - AKOS)
Use case	Natural hazard - Floods
Description	Floods usually occur due to heavy or prolonged rainfall, rapid snow melting or a combination of factors. The fundamental causes of floods are precipitation conditions, relief features, vegetation, rock and other characteristics, but floods are increasingly also a consequence of human intervention in nature. Floods cause fatalities, economic losses, social changes and environmental consequences. The damage to flooded areas is extensive. Homes and other property can be lost. People can lose their jobs. Ultimately lives too. Floods that can cover areas where infrastructure is located on the ground with water, also in connection with landslides, the removal of a certain part of the land. Due to climate changes the risk of floods is raising. In Europe we are challenging a lot of weather conditions where rivers are flooding. In Slovenia there are also many possibilities of flooding in some areas. In this use case, we predict a condition that there has been heavy rain for at least 3 days. Also, it is high spring and early summer so snow in the mountains is melting as well. The weather report is bad and there was raised an orange alarm for floods by governmental institution for water surveillance for almost all area in the country. The water level is rising rapidly. In floods, the main risk of this accident, for electricity sector is that water cause damage to facilities of electricity grid that are located on the area near rivers. The highest risk is to the transmission system substations, especially to the control and command rooms which are located on the ground and can therefore be flooded. The substation can operate even if it is flooded, unless the propulsion and control devices are also flooded. In addition to substations, the power line stands are also at risk due to the floods. Several facilities are located in flood areas of larger rivers that could be flooded by a flood wave caused by a dam collapse, but the probability of such an event is very small. Eles's infrastructure is not at risk due to rising sea water. Due to the floods and damage to telecommunication facilities and equipment, the communication can be interrupted. Stationary and/or mobile phones are not working. There is a challenge to communicate with important stakeholders and rescue teams. In the case of digital, the floods can submerge infrastructure located on the ground, disrupt underground cabling, and cause landslides that physically remove terrain.

	The events (flooding in 2023) also exposed the importance of cross-sectoral coordination and dependencies on other sectors such as energy and transport, especially in remote and mountainous regions. The objective is to highlight operational vulnerabilities.
Damage	**Structural:** Physical destruction of buildings, base stations, and cable routes. Some underground optic cables were affected by landslides or floodwaters. Physical destruction of buildings and infrastructure (transmission system substations, power line stands). The consequence of a flood may be the failure of a substation. **Functional:** Disruptions in field maintenance operations, mobile access, and service restoration activities due to impassable roads or lack of fuel. Several remote locations were cut off, leading to significant delays in restoring service. Dependencies on energy providers and coordination with government ministries (e.g., for logistics support) proved to be a critical challenge. Interruption of essential services – transmission of electrical power, and consequently distribution of electricity to the consumers on the area of floods. Due to pollution also material damage to facilities and equipment can be caused that can result in prolonged operational incapacity. In the event of an internet outage, the monitoring function may be hindered or impaired. In the event of (longer) internet or power outage, the monitoring function may be hindered or impaired. Notification and warning systems would not be accessible, making it difficult for the authority to operate. **Economic:** Financial losses due to service outages, emergency repair costs, and contractual penalties. Significant costs also arose from temporary solutions like mobile base stations and power generators. **Social:** Inability to provide services to first responders, municipalities, and citizens, especially in areas with no alternative communication channels. Mobile networks are the only available communication method in many rural areas. Effects on people's health and safety. Floods can cause harm to people that are on the area of flooding in that moment. A lot of houses and interiors can be damaged by water. Without electricity there is no lights, heating, warm water, almost all equipment in houses needs electricity to operate. Some employees might not be able to come to work nor connect remotely as they lose internet connection. There could be delays in informing or warning the public about cyber threats, as well as in responding to incidents and threats, which could consequently greatly increase the damage. **Environmental:**

	Additional environmental risks arose from emergency actions, such as deploying diesel generators in protected areas or inaccessible zones. Negative impacts on ecosystems.
TO BE Future situation (after ENDURANCE)	
HOW	ENDURANCE can significantly contribute to improving the quality and harmonization of Risk Assessment implementation both at the level of Competent Authorities and individual Critical Infrastructure (CI) Operators. **Architecture** Even if the system is a centralized solution, it is also highly distributed. Key elements of the whole architecture solution consist of: • National centralized technological provider • National, regional, and local providers of CI resilience data – if necessary • National CI coordinators – which collects key data • CI operators • data portals for public • Open data sources for CI operators and coordinators Basic entities of the architecture for our pilot consist of CI operators and national coordinators. However, in general, the whole architecture ecosystem includes also other entities, which are national center for crisis management (NCKU), emergency number 112 centers (PSAP), open data portals (for data retrieval), and public web portals and media portal (for informing the public). The architecture can be seen as layered system consisting of local, regional and national layer. One operator (or multiple) for the whole country, which manages the technological solution. Such solution is highly centralized on the national level; however, some part of centralized solution can be even on regional levels. We need at least one technological operator, which collects data from all the CI. National CI supervisor uses functionalities from the technological solution provider. Each CI entity can have many input parameters, however, only subset (or aggregated) (in short: key parameters) of data is sent toward centralized technological solution. The final technical solution should provide clear view of situational awareness. This is valid for both the entities itself, and for the national (or even regional or local) point of view. **To increase the resilience in the case of flooding** The main focus of the pilot is to increase the resilience for the case of natural disaster, which is flooding. That would be achieved by monitoring, data and decision managing, increasing situational awareness and exchanging relevant information. This will be supported by real scenarios for different cases (scenarios and sub scenarios) of flooding.

	Due to climate changes the risk of floods is raising. In Europe we are challenging a lot of weather conditions where rivers are flooding. In Slovenia there are also many possibilities of flooding in some areas. The main scenario, we predict a condition when there has been heavy rain for at least 3 days. Also, it is high spring and early summer so snow in the mountains is melting as well. The weather report is bad and there was raised an orange alarm for floods by governmental institution for water surveillance for almost all area in the country. The water level is rising rapidly. The scenario would like to expose the importance of cross-sectoral coordination and dependencies on other sectors such as energy and transport, especially in remote and mountainous regions. The objective is to highlight operational vulnerabilities. For electricity sector the water can cause damage to facilities of electricity grid that are located on the area near rivers. The highest risk is to the transmission system substations, especially to the control and command rooms which are located on the ground and can therefore be flooded. The substation can operate even if it is flooded, unless the propulsion and control devices are also flooded. In addition to substations, the power line stands are also at risk due to the floods. For telco (digital) sector the floods can submerge infrastructure located on the ground, disrupt underground cabling, and cause landslides that physically remove terrain. Foods can affect remote base stations and rural access networks, where access can be limited or completely cut off. In short, the telecommunication facilities, equipment, and the communication can be interrupted. Stationary or mobile phones cannot work. Challenge can be, to communicate with important stakeholders and rescue teams. **Technologies** Basic technologies used would be Risk Management, AI and Digital Twin. In addition, technologies such as the use of open data, web technologies, cloud technologies, will also be used. Appropriate technological support in the field of Virtual Reality and Serious Gaming will bring added value in conducting both small- and large-scale exercises aimed at enhancing preparedness and responsiveness to ensure the continuity of operations across various Critical Infrastructure (CI) capabilities. **Scenarios** The basic idea is to cover natural event, which is flooding. With the aim to cover both the big event, and other sub-scenarios. This way, we would cover as many key situations related to floods as possible. Whereby the scenarios and actual events can be implemented at the local, regional, or national level. All these scenarios and sub scenarios are also the basis for Digital Twins and Simulation games. The scenarios and sub scenarios would like to cover (but it is not limited or total defined by):

- the main scenario, where there is heavy raining for 3 days (with high level of water before that last event), which causes flooding all over the country.
- Fat raising of water in one of the main cities in Slovenia, covering both minor rise in river levels with minor flooding, and also major rise in river levels with major flooding in the city.
- One region covered under water (could be for one or five days)
- One small local area covered by hard raining, making a lot of damage, which ca be of flooding, landslide and other damages due to the event.

Situational awareness

Within the control room are provided tools to help increase situational awareness.

Elements to increase situational awareness are map, DSS (Decision Support Systems), risk management evaluation, use of different scenarios and simulation games, and AI (Artificial Intelligence).

The first thing to have, is a picture of the infrastructure. A map of the geographic area, where the data is, to be used with the infrastructure map, and to see where there is any infrastructure that may be at risk from flooding, is that first step.

Monitoring of input data, supported by good dashboard, which shows all the relevant information about situational awareness in one place is the most important thing. The second most important point should be a solution that supports the decision support system.

The next important technological solution that can significantly contribute to improving situational awareness regarding the status and functioning of individual infrastructures, as well as their potential interdependencies and cascading effects, is reflected in the use of Digital Twin technology.

Methodologies covered

The use of a unified methodological framework supported by appropriate Artificial Intelligence will standardize and accelerate Risk Assessment processes. A proper risk analysis forms the essential foundation for a unified understanding, situational awareness, and structured and transparent planning for the implementation of risk management measures.

Basic methodology guideline will be provided by ISO 23001 (BCMS) procedures (business continuity). If needed, ISO 27001 for cyber security is also taken into account.

KPIs

The point of KPIs is that they define key levers for controlling events. Key KPI are provided as main data for managing the events in efficient way.

The parameters for KPI will follow the guidelines what will be the damage, what will be the downtime, and what are the damage risks.

Key KPIs are derived from what already exists and is held by national coordinators, by supplementing them with parameters that are recognized as important in this segment.

	Subset of key data or aggregation of data could be provided to national center for crisis management or for public (like on PSAP or public web or media portals). The main guideline when informing the public is what the public gains from it. Support for KPI will be based on core data profile.
Interaction	In the planning and analysis phase, support for the scenario can be used through methodological steps for Support for Resilience Planning, Continuous Resilience Improvement, and Awareness & Training. Current steps in planning and risk analysis, as well as subsequent training, remain overly static and are not supported by technological capabilities. In this area, ENDURANCE can make a significant contribution to improving the understanding of the actual situation and can notably accelerate the processes. The key step forward of this pilot scenario is to ensure real time-based monitoring of the danger, which is capable to handling of given danger in a way that is more dynamic capable. In such a way the proposal would increase the resilience. In the field of situational awareness and direct coordination, it is necessary to identify modular approaches for integrating ENDURANCE technologies with those already in use for operational monitoring of situations, coordination, and response to crisis conditions, as well as for mitigating the consequences of crises affecting the functioning of critical infrastructure. All these elements are key factors for significantly increasing the resilience of critical infrastructure and the continuity of essential services.
Data	Based on the needs of each specific technology, the scope of concrete data sources required for proper testing of the technologies in the Slovenian pilot will be defined. **Data structure** Data will be defined and used as JSON structure, which is de-facto standard for data definition and exchange. Typically, CSV format would also be used. **Types and sources of the data** Data used will be of three types: historic data, real time data, and synthetic data. The latter will be generated for some sub scenarios, simulation games and Digital Twins (DT). Historic and real time data will be provided from open data portals, like ARSO and Meteo.si, and will include different weather parameters (like rainfall and temperature) for different locations (through whole country). The list of open data includes meteo.arso.si, gis.akos-rs.si, podatki.gov.si, but it is not limited only to them. Some data will be provided, if necessary, from CI operators or national coordinators. Regarding the data, it to be addressed: which data are really needed, how to detect them and how to present them, from the data set, which of them are the most important. **Open data**

	For cases involving natural events, such as floods, it is possible to use open data. This is also the case in this case. The use of river flow data and various weather data is envisaged. For the example of river flows, it is planned to use data on river water level and flow. For weather data, it is planned to use several different weather parameters, such as temperature (current, maximum, minimum), cloudiness, air pressure and precipitation. To obtain the most realistic picture possible of what is actually happening in nature, data will be obtained in real time from various locations throughout Slovenia. For river flows along various rivers stations (Mura, Drava, Ljubljanica, Sava, Savinja, Krka) stations throughout Slovenia. The same weather parameters will also be obtained from various weather stations (like Celje, Ljubljana, Postojna, Maribor, Koper, Kranj, Novo mesto) throughout Slovenia. **Core data profile** Based on existing experience, a core set of parameters will be proposed. The core data profile will consist of all the main parameters that need to be covered to provide the information about the danger and the situation. Core data profile will be used by both CI operators and national coordinators. Not just for recording of data itself, but also for the data exchange and data storage on long term. Additionally, core data profile could be for CI operator provided for greater granulation. In this way, it would help them to increase the resilience by managing more information about their situational awareness.
Constraints and restriction	A certain portion of the data will only be available in historical form. No sensitive data will be retrieved.

3.2.2 MESO PILOT ROMANIA

Organization	Romania, 2 CI sectors (Digital and Health): 2 national and sectorial authorities (National Authority for Cybersecurity - DNSC; Romanian Ministry of Health - MoH), 1 CI operator (General Directorate for Internal Protection - DGPI), and 1 Health SME (Dr. Muntean Clinic - CGDM).
Use case	Natural hazard + Human intervention (malicious): Earthquake, followed by downstream, cascading side effects on critical entities/services
Description	Seismic event (earthquake) that could damage physical infrastructure, disrupt power and connectivity (and thus the capability to communicate with the population), and render key facilities inoperable. Secondary concerns include structural damage to data centers, cooling system failures, and staff unavailability as authorities will be focusing on the earthquake event & cyberattacks arising on national authorities which are working in risk management. At the same time, the earthquake and its potential aftermath will put significant pressure on crisis management and rescue operations.

	Seismic event, specifically an earthquake, has numerous potential implications and cascading effects with significant impact on various services and sectors within the national Romanian infrastructure, including the health and digital sectors, both at the physical and virtual levels. Such an event poses significant risks, including damage to critical facilities, disruption of power and connectivity, and the inoperability of essential services. Key concerns include the structural integrity of data centers, potential failures in cooling systems, and the unavailability of staff. During such crises, authorities will prioritize efforts civil protection efforts, which may divert resources and attention from other critical areas, including cybersecurity threats to national infrastructure. This could hinder the existing plans and strategies necessary for restoring the civil ecosystem. We must also consider the impact on hospital coordination. Certain regions may experience heightened effects post-earthquake, necessitating effective triage and enhanced collaboration among medical facilities in proximity to the event. It is crucial to recognize that general coordination efforts may be impeded during this time. Finally, power outages must be considered as specific risks associated with an earthquake, as any disruptions to the electricity supply can lead to a cascading effect across various sectors, including healthcare, transportation, and digital services (CNAS). ---------- After a major earthquake, local datacenters will be affected; power outage in hospitals – electronic patient records are inaccessible. Surgeries may be put on hold due to this scenario. Reaction time is impacted, as patient records may need to be filled in manually, as the digital ones will be unreachable. Risk of mal-praxis, increased death-toll, and permanent loss of medical data of patients. Some hospital sections could become overcrowded, thus unresponsive (intensive care unit, emergency unit, etc.). Any interference by a malicious external actor serves to further complicate the situation, create and/or exploit breaking points, disrupt the crisis management decision-making system, and leverage any indecision on its part in disinformation narratives that support the strategic objective of eroding public trust in the authorities. After an earthquake, local data centers can be affected due to power outages in hospitals, damage to equipment integrity, or a combination of both, resulting in heightened risks, such as: Impact on Medical Services: Access to electronic patient records and related files will be compromised, leading to immediate repercussions for Intensive Care Units (ICUs) and other emergency departments. This may result in both scheduled and unscheduled medical interventions being postponed or entirely halted until effective mitigation strategies are implemented. Consequently, surgeries may be delayed. Permanent Loss of Medical Data: The potential for irreversible loss of critical medical data and records poses a serious threat to patient care continuity. Slower National Coordination: The ability to coordinate effectively between hospitals at the national level will be diminished, hindering collaborative efforts during crises.

	Increased Response Times: Response times may be adversely affected as medical records will need to be filled out manually, given that digital systems may be inaccessible. Even though various plans, such as triage protocols and transportation to nearby facilities, are currently established to varying degrees, vital medical services may still face significant delays, and if the crisis prolongs, they can stop completely. Finally, we must consider the risk of exposure for digital infrastructure, as malicious actors can exploit the prevailing crisis to launch cyberattacks. This could lead to the exfiltration or permanent destruction of critical data from the digital systems of national authorities.
Damage	**Structural Damage**: Physical destruction of buildings, medical equipment and infrastructure. **Functional Damage**: Interruption of essential services (healthcare and afferent digital systems upon cyberattack initiation). **Economic Damage**: Financial losses and repair costs. **Social Damage**: Effects on people's health and afferent care services. **Environmental Damage**: Negative impacts on ecosystems. **Reputational Damage**: Negative impacts on trustworthiness of essential services and their providers. Public perception risks: Eroded/diminished trust in authorities. **Level of readiness risks**: Reduced readiness of own/allied defence forces readiness
TO BE Future situation (after ENDURANCE)	
HOW	ENDURANCE aims to enhance resilience planning through strategic recommendations supported by digital twin technology. To this effect, we aim to facilitate the upload of user profiles and implement an early warning system via a comprehensive dashboard for critical infrastructure systems. Meaningful scenarios will be produced in case of a major event, and through scenario testing, we will provide risk scores and resilience assessments, including an interdependencies indicator.
Interaction	We aim to implement warning and early warning systems to address events that may affect critical services, including the digital and health sectors. This allows us to build ecosystem resilience awareness and properly address the impact on cross-sector services.
Data	To facilitate the development of models required by the digital twin technology, we aim to attain a thorough understanding of alternative power sources and their cascading impacts on the digital and healthcare sectors.
Constraints and restriction	Accessing resilience-relevant data of critical infrastructure in real time can present challenges. To facilitate this process, it is essential to identify and engage the appropriate national and European structures that can mandate the integration of automatic resilience assessment technologies, such as those developed in the ENDURANCE project, into regulatory practices.

3.2.3 MICRO PILOT ITALY

Organization	Insiel S.p.A. / Regione FVG, Italy, Public Administration are the two main actors of this pilot. The Friuli Venezia Giulia Region is and Authority and the owner of Insiel, that is the company that provide ICT services to all public entities in the regional territory.
Use case	Cybersecurity - Human sabotage of Datacenter's Safety systems People with malicious intent damage the safety system of the Datacenter's building in order to create harm to people and assets.
Description	The use case is regarding the human disruption of the Datacenter's Safety systems via cyber-sabotage. Threat actors will trigger some false alarm to force the workers to leave their workstation unattended. The threat actors also might activate the remotely by a cyber-sabotage the safety system or disable it to cause harm to people that works inside Datacenter building and made the data and services managed by the server hosted by Datacenter useless or not unattended.
Damage	**Structural Damage**: Physical damage to asset hosted by datacenter. **Functional Damage**: Interruption of the services hosted by the server in datacenter. Potential stealing of information. **Economic Damage**: interruption of the services hosted by the servers and disruption on the public administration operations. **Social Damage**: disruption on citizens activities based on public administration operations and this could cause social anxiety and public dissatisfaction. **Environmental Damage**: eventually some gas and material freed in the datacenter activated by a safety system sabotage could cause environmental damage to assets and server rooms.
TO BE Future situation (after ENDURANCE)	
HOW	Improve the detection and the response capabilities through simulations and training. Evaluate the impact on services provided to citizens and companies (generic PA & Health) through Digital Twin and Simulation methodology. Enabling the identifying data layers and "sensors" like network usage, anomaly detections, etc. Monitoring of efficiency in normal conditions and "under attack". Evaluating capacity of reaction and restore of critical services. Identifying bottlenecks and provide policy recommendations. Identifying and assess the interdependencies with other sectors.
Interaction	Integrate specifics training that include the cooperation of different area of the same organization. Provide insight on how the crisis can evolve and how this crisis can impact on the organization assets at the AS IS and provide feedback on how the current cybersecurity measure could be improved in order to better face the crisis.

Data	Reports and insight on how improve the current status of the safety systems monitoring. Playbook containing the mandatory activities that need to be undertaken during a sabotage on safety systems.
Constraints and restriction	Yes. We need to improve the cooperation between different areas of the organizations. Also the sharing of the data could be difficult.

3.2.4 MICRO PILOT GREECE

Organization	Greece, 2 CI sectors (Drinking Water, Wastewater Management) 2 regional authorities (Regional Development Fund of Attica-RDFA, Regional Development Fund of West Greece- RDFW), one CI operator (EYDAP)
Use case	Natural hazard: Prolonged Drought causing drinking water supply shortages due to water reservoir depletion and supply interruptions
Description	This use case addresses the critical challenge faced by CI operators and regional authorities in managing water supply during prolonged drought periods. Due to climate change, droughts have become increasingly common in Greece, creating significant operational challenges for water management. The scenario involves managing both drinking water and wastewater subsystems during water scarcity conditions, requiring coordinated response strategies to ensure continuous service delivery while minimizing impact on consumers.
Damage	**Functional Damage**: • Interruption of essential water services with scheduled supply interruptions (2-3 hours daily during severe drought periods) • Compromised wastewater treatment operations • Reduced water pressure and quality concerns **Economic Damage**: • Increased operational costs for alternative water sourcing • Revenue losses due to service interruptions • Investment requirements for emergency infrastructure • Consumer compensation and regulatory penalties **Social Damage**: • Public health risks from inadequate water supply • Disruption of daily life activities (cooking, hygiene, business operations) • Increased social tension and public dissatisfaction **Environmental Damage**: • Ecosystem stress from over-extraction of remaining water sources • Potential contamination of alternative water sources • Long-term impact on regional water table and biodiversity

	.
TO BE Future situation (after ENDURANCE)	
HOW	ENDURANCE can provide an integrated forecasting and decision support platform that transforms how water management organizations prepare for and respond to drought conditions. Rather than attempting impossible long-term weather predictions, the platform focuses on scenario-based simulation capabilities that allow operators to explore various drought conditions and test different response strategies in a safe virtual environment. Training and Exercises based on potential simulation scenarios can help with coordination between involved stakeholders (operators and regulators) and ensure personnel's ability to respond to a crisis. The technology framework should combine AI-powered climate scenario modeling specifically tailored to catchment areas of interest, with sophisticated usage analytics that can differentiate between irrigation, industry, municipal, and household consumption patterns. This integration enables water managers to understand how different drought scenarios might cascade through various consumption sectors and test intervention strategies before implementing them in real-world conditions.
Interaction:	**Inside the organization**: Creating integrated dashboards for cross-departmental coordination, automating routine monitoring tasks, enabling predictive maintenance scheduling, and providing decision support tools for crisis management. **Outside the organization**: Coordinating with other CI operators and authorities through the Trusted Data Space and enabling real-time data sharing with regulatory authorities.
Data	• Long-term climate data for reservoir areas (10–20-year forecasts) • Sector-specific water usage data (irrigation, industry, municipal, household consumption patterns) • Hydrological modeling data for the reservoirs • Cross-sector demand correlation data for predictive modeling • Economic and demographic data for long-term consumption trend analysis
Constraints and restriction	The most probable barriers are a lack of accurate hydrological and climate data for reservoirs, budget and personnel training constraints that can hinder long-term efforts and cooperation between stakeholders.

4 Workshop reports

The initial phase of WP1 focuses on evaluating the current frameworks, definitions, and methodologies related to Critical Entity Resilience (CER). This includes defining essential services, identifying critical entities, and analyzing risk assessment methods, interdependencies, and cascading effects. Data collection during this phase is conducted through desk research, targeted expert surveys (where relevant), and a series of local workshops held in the pilot countries Slovenia, Romania, Italy, and Greece within the first three months. These workshops facilitate direct engagement with critical infrastructure stakeholders to gain practical insights into existing challenges and effective practices.

Additionally, a broader European-level workshop, held in Month 6, enabled cross-border knowledge exchange and reinforced findings from the national consultations. Together, these workshops have played a vital role in strengthening stakeholder relationships, promoting the exchange of expertise and best practices, and gathering critical input for the development and co-creation of ENDURANCE project outcomes. This early phase of enhanced strategic dialogue and collaboration has accelerated the identification of gaps and challenges, while fostering coordinated, efficient solutions to improve collective resilience against disruptions. The following subchapters provide a detailed summary of key conclusions drawn from each national and European workshop.

4.1 Local workshop in Slovenia

Event Title: National Workshop of the EU Project ENDURANCE: "Seeking Appropriate Solutions to Ensure Increased Resilience of Critical Infrastructure"

Co-organizers of the event: Slovenian partners in the ENDURANCE project (Institute for Corporate Security Studies, ELES, Telekom Slovenije, AKOS, URSIV, Silver Bullet Risk)

Event date and time: Wednesday, November 27, 2024, from 09:00 to 13:00.

Location: Conference Hall, ELES Technology Center, Beričevo 70, Dol pri Ljubljani.

Key Objective
The challenges posed by a complex security environment, including various security threats, call for a content-driven workshop focused on finding appropriate solutions for developing a resilient ecosystem that ensures the necessary level of resilience for our key organizations and systems. The ENDURANCE project is dedicated to exploring new methodological, procedural, and technological steps in enhancing the resilience of critical infrastructure. To implement the necessary steps in the project, it is essential to gather information on real-world experiences, challenges, current conditions, existing gaps, and best practices in ensuring the resilience of organizations and society as a whole.

Given that the security environment and the risks we face are becoming increasingly complex, it is essential to find appropriate solutions that are modular in nature and embedded within a sufficiently flexible security system, allowing for effective threat response.

The primary goal of this workshop is to facilitate open discussions and seek positive conclusions to support EU strategic institutions in identifying effective approaches for developing a dynamic security ecosystem aimed at enhancing the resilience of critical infrastructure operations.

Present organizations

Representatives: ICS Ljubljana, ELES, Telekom Slovenije, Silver Bullet Risk, Agency for Communication Networks and Services of the Republic of Slovenia (AKOS), Government Information Security Office (URSIV)

Elektro Gorenjska (DSO), Water supply company city of Maribor, University Clinical center Ljubljana, Traffic Institute/Slovenian railways, Telecommunication operators: T-2, Telemach Slovenije, A1 Slovenija, Ministry of Defense, Slovenian Corporate Security Association.

4.1.1 Summary of responses from discussions

In this report from the conducted workshop, we have gathered all the key highlights of the discussion and tried to synthesize it in a way that the report does not lose important information related to the specificities of sectors as well as the common conclusions in each part. The discussion was, in some parts, based on the structure of the questionnaire, while in other parts it expanded the boundaries beyond the topics defined in the questionnaire. For this reason, we are presenting the workshop record separately from the analysis of the questionnaires. The questionnaire example is provided as an appendix 2 to this document. The comprehensive record of various factors and proposals seems important in this first phase of information gathering, as the broader context of information would be useful for work in other WPs, where the specifics will form important starting points for continuing the research process.

Questionnaire results and interpretation

DISCUSSION PANEL 1

Insights of interested parties on CI – resilience in specific CI sectors (existing policies, strategies, standards, SOPs, best practices, and business continuity plans identified and/or adopted by CI authorities and operators).

Resilience Concept

Resilience Concept refers to the ability of systems, organizations, communities, or individuals to adapt, withstand, and recover from disruptions, crises, or unexpected changes. Resilience includes:

1. **Risk anticipation** – identifying and assessing potential threats and vulnerabilities.
2. **Preparation and planning** – establishing strategies, policies, and measures to reduce the impact of disruptions.
3. **Response and adaptation** – reacting quickly and effectively to crisis situations.

4. **Recovery and learning** – restoring normal operations and improving preparedness for future challenges.

In the context of critical infrastructure (CI), resilience means ensuring the continuous operation of essential services, even in the event of disasters, cyberattacks, or other threats.

Through the analysis of the collected responses from participants, we have identified the following key aspects of defining resilience:

- **How would you define the concept of resilience in the context of your organization or sector?**
  - Resilience refers to ensuring secure and continuous operations (maintaining the safe and uninterrupted functioning of networks, systems, services, and data security) despite external threats and internal vulnerabilities.
  - Resilience is the ability of an organization to anticipate, prevent, respond to, and recover from disruptions or threats while maintaining key functions and ensuring the seamless provision of services.
  - For our organization, resilience means a set of activities aimed at preventing or managing potential disruptions or interruptions in the delivery of essential services. It involves both risk management processes and the implementation of technical and organizational measures to prevent extraordinary events or respond to them and mitigate their impact as quickly as possible.
  - Ensuring uninterrupted operations even in crisis situations that affect our CI or interconnected (interdependent) CI. This includes providing healthcare services, digitalization and data security, connectivity with other sectors, and maintaining trust in the healthcare system. The critical infrastructure of healthcare is therefore essential for ensuring high-quality medical care, safety, protection, and societal stability. Awareness of its importance enables better planning, protection, and response to various threats.
  - The ability to operate and maintain business continuity in extraordinary, unforeseen, and critical conditions.
  - The ability of an organization to survive and quickly recover from disruptions and crises.
  - Ensuring the highest possible level of operation under all conditions.
  - The capacity to respond rapidly to potential disruptions and quickly return to normal operations.
  - Implementing technical, organizational, and operational measures and controls to effectively address challenges, disruptions, and crisis situations.
  - Ensuring an uninterrupted supply of electricity, regardless of various external and internal influences.
  - Ensuring the smooth operation of services, maintaining the security and stability of communication networks and information systems, and delivering services to end users.

- **What does resilience mean to you in the context of critical infrastructure operations?**
  - In this context, resilience refers to ensuring the secure and continuous operation of those parts of networks, systems, and services, as well as data sets that are identified as critical, despite external threats and the exploitation of internal vulnerabilities.
  - The resilience of critical infrastructure means ensuring uninterrupted operation despite natural disasters, cyberattacks, or technical failures of critical entities or CI operators. This includes preventive measures, crisis response, and strategies for rapid recovery.

- Resilience means, first and foremost, ensuring infrastructure security through controlled access and proper maintenance to prevent potential technical issues. At the same time, it involves implementing measures that ensure that, even in the event of a failure of a critical infrastructure component, we can still supply electricity to our users and, consequently, to end consumers, including businesses and households.
- Resilience is the ability of a system, organization, community, or individual to adapt, recover, or continue functioning after difficulties, disruptions, or crises. It involves managing and overcoming challenges while maintaining functionality even in difficult conditions. Resilience includes both preparedness for potential crises and the ability to recover quickly when issues arise.
- Simply ensuring the continuous supply of safe drinking water to consumers.
- The ability of digital services to function or recover quickly in the event of an emergency.
- The ability to operate continuously under all conditions.
- Quick responsiveness to disruptions and a rapid return to normal operations.
- Regular electricity supply, fuel provision for generators, security assurance, and sufficient personnel in case of major outages.
- The ability to provide electricity for the operation of other sectors.
- The capability of systems to withstand disruptions (floods, cyberattacks, etc.), quickly adapt, and restore key functions after an incident.

Sector operator / legal representative:

- **Please specify the sector you operate in and briefly describe the main activities of your organization related to the resilience of critical infrastructure.**

In this context responders indicated sectors from which they are coming:

- energy (electro-energy)
- Telecommunication
- Drinking water supply
- Transport (rail + road)
- Public sector (governmental organizations-regulator for CER, Telco and cyber security)

- **What are the potential risks or consequences if the principle of resilience is not properly applied in your organization or sector?**

- The risk of a complete failure of the mobile and fixed network, failure to provide emergency calls, and general communication breakdown.
- Disrupted electricity supply.
- In case of an outage, a significant number of residents may lose access to mobile and fixed services.
- Disrupted transportation connections, interrupted freight transport, economic damage.
- Service interruptions, failure to provide services, data exfiltration, violations of operational procedures.
- The greatest risk is when one part of critical infrastructure fails, leading to cascading effects.
- Disruption of water supply, potential contamination of consumers, cascading effects on other critical sectors.
- Potential risks include outages or disruptions in electricity supply to the population and economy, with consequences depending on the scope and duration of the outage.

- Disruption of communication services, loss of trust from users and partners, legal penalties for non-compliance with regulations, increased costs due to uncontrolled disruptions.
- Ignoring resilience principles could lead to worse performance or failure of networks, systems, and services, as well as compromised data security.

Resilience area:

- **Cyber, physical, human domain – please prioritize the types of risks for your resilience and, where applicable, highlight the interconnections between these risk domains in your sector.**
  - Natural events (earthquakes, floods),
  - Technical risks,
  - Security risks (physical, cyber),
  - Cyber risks related to geopolitical situations and technological advancements,
  - Human risks (lack of experts),
  - Cyber threats, workforce shortages, physical threats,
  - Cyber domain, physical domain, human domain,
  - Cybersecurity, physical security,
  - Physical protection of critical infrastructure,
  - The cyber domain and the risks it poses,
  - Hybrid risks, increasingly present due to changes in geopolitical global conditions,
  - Physical domain,
  - Cyber threats (e.g., network attacks, malware); natural disasters (floods, fires); technical failures,
  - In our company, we manage all types of risks: external power outages, equipment failures, risks related to employees or people, cyber risks, risks related to physical and fire safety, risks concerning suppliers and data processors, and others. Humans (employees, clients, external individuals) are always at the forefront, either as a source of risk or responsible for managing the risks.

Legal framework

- **Please list the main policies/directives (local, national, international) that govern your organization's activities related to resilience.**

  - The Critical Infrastructure Act (ZKI)
  - Regulation 2019/941/EU on risk preparedness in the electricity sector
  - Disaster Protection Act (ZVNDN)
  - Fire Protection Act
  - Occupational Health and Safety Act (ZVZD-1)
  - Information Security Act (ZInfV)
  - NIS2 Directive
  - Electronic Communications Act (ZEKOM-2);
  - General Act on Incident Reporting and Evaluation, and Announcing Limitations or Disruptions, as well as the General Act on Additional Security Requirements (still under adoption)
  - Additionally, we consider the recommendations and guidelines of other relevant institutions (e.g., ENISA)
  - CER Directive
  - GDPR Directive
  - AI directive

- DORA directive.

- **Please list those that are strictly related to the sector your organization belongs to.**

  - Zakon o oskrbi z električno energijo (ZOEE),
  - Uredba 2019/941/EU o pripravljenosti na tveganja v sektorju električne energije
  - Načrt pripravljenosti na tveganja v sektorju električne energije
  - Omrežni kodeks za kibernetsko varnost čezmejnih pretokov električne energije (NCCS)

- **Who are the reference authorities for your organization regarding resilience (local or national level)? And how should communication with the authorities be handled? Is there a standardized coordination procedure?**

  Organizations:

  - Ministry for Environment and Energy (MOPE),
  - Ministry of Defence (MORS),
  - Information Security Office (URSIV);
  - Ministry of Digital Transformation
  - Ministry of the Interior (MNZ), and the Police,
  - Slovenian Holding for management of companies in public ownership (SDH)
  - Agency for Communication Networks and Services (AKOS),

  Procedures:

  - Communication procedures are standardized and aligned as stipulated by legislation.
  - Telekom Slovenije uses standardized reporting and coordination procedures for crisis response and compliance.
  - National Plan for Responding to Cyber Incidents (NOKI).

Standards and SOP (standard operational procedures)

- **What are the standards for your organization? Which ones are mandatory? Which are optional but used in your organization? (e.g., ISO 27001 or others)**

  - Mandatory standards: **ISO 9001**: Quality Management System, **ISO 14001**: Environmental Management System, ISO 45001: Occupational Health and Safety Management System, **ISO 27001**: Information Security Management System, **ISO 55001**: Asset Management System.
  - Optional but used standards: **ISO 31000**: Risk Management, and **ISO 22301**: Business Continuity Management System.

- **Do you conduct internal and/or external audits regarding compliance with these standards or directives? How often are these audits carried out, and what are the key findings?**
  - Internal audits are conducted once a year.
  - Annual compliance checks by external auditors in accordance with the awarded certifications.

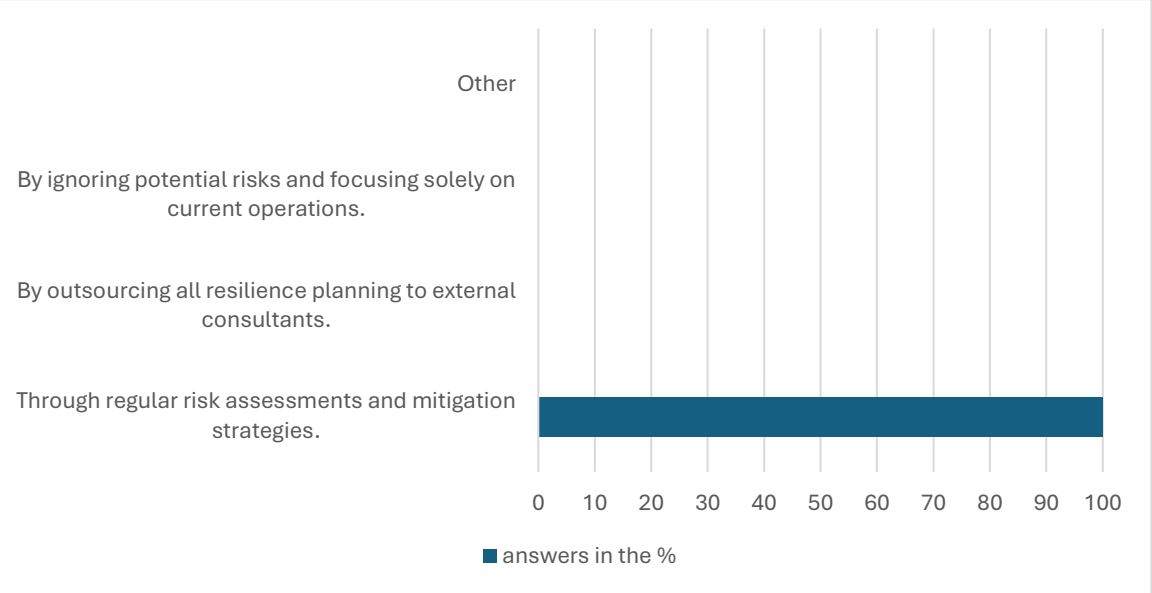
- **Do you have any written and officially approved guidelines or procedures that complement these standards?**

- Directives: DORA, NIS2, CER, NIST 800-xx
- Internal regulations and policies
- Requirements of sector-specific legislation
- Internal policies
- In preparing the documented information security management system and business continuity management system, we have relied on external consultants.

Modus operandi

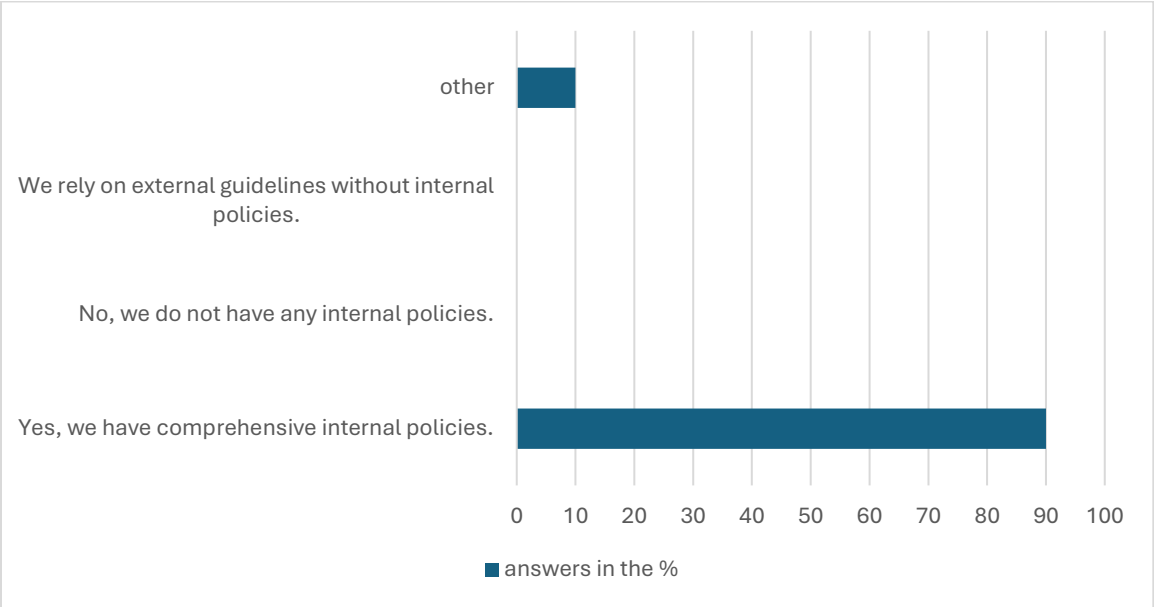
How is resilience included in the strategic or operational planning of your sector?

- ☐ Through regular risk assessments and mitigation strategies.
- ☐ By ignoring potential risks and focusing solely on day-to-day operations.
- ☐ By outsourcing all resilience planning to external consultants.
- ☐ Other



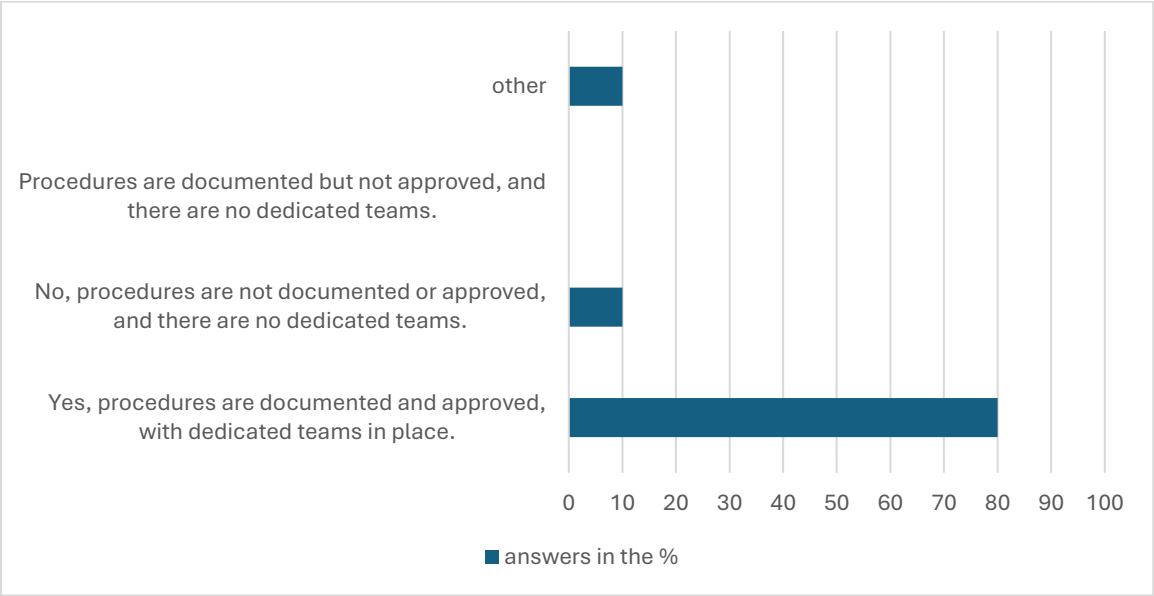
How is resilience included in the strategic or operational planning of your sector?

- ☐ Through regular risk assessments and mitigation strategies.
- ☐ By ignoring potential risks and focusing solely on day-to-day operations.
- ☐ By outsourcing all resilience planning to external consultants.
- ☐ Other...



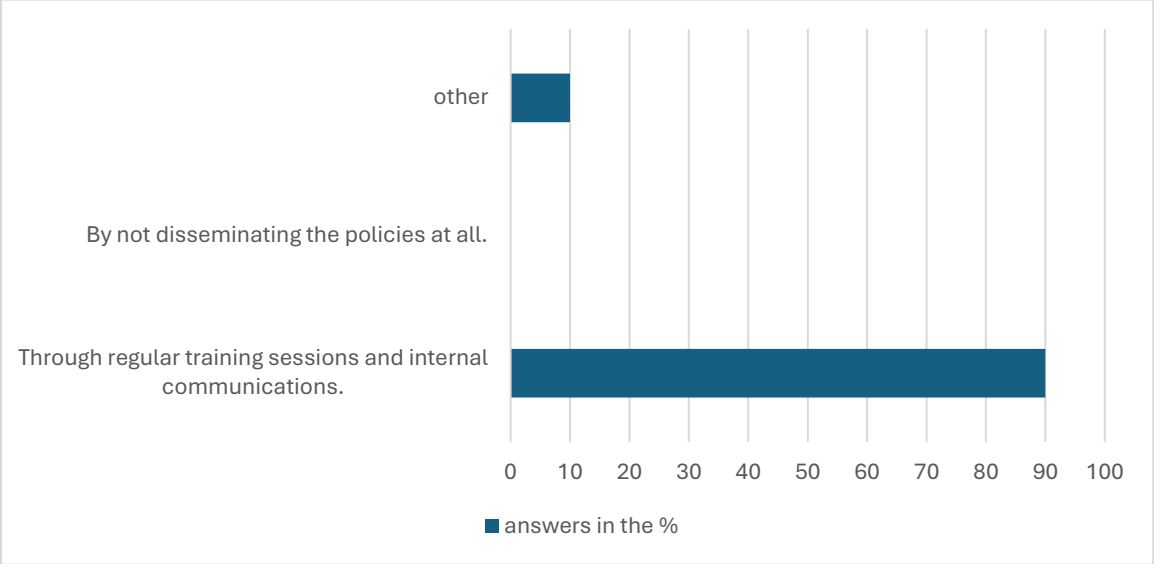
Are the procedures documented and approved? Are there specialized departments or dedicated teams responsible for resilience efforts?

- ☐ Yes, the procedures are documented and approved, with dedicated teams.
- ☐ No, the procedures are not documented or approved, and there are no dedicated teams.
- ☐ The procedures are documented but not approved, and there are no dedicated teams.



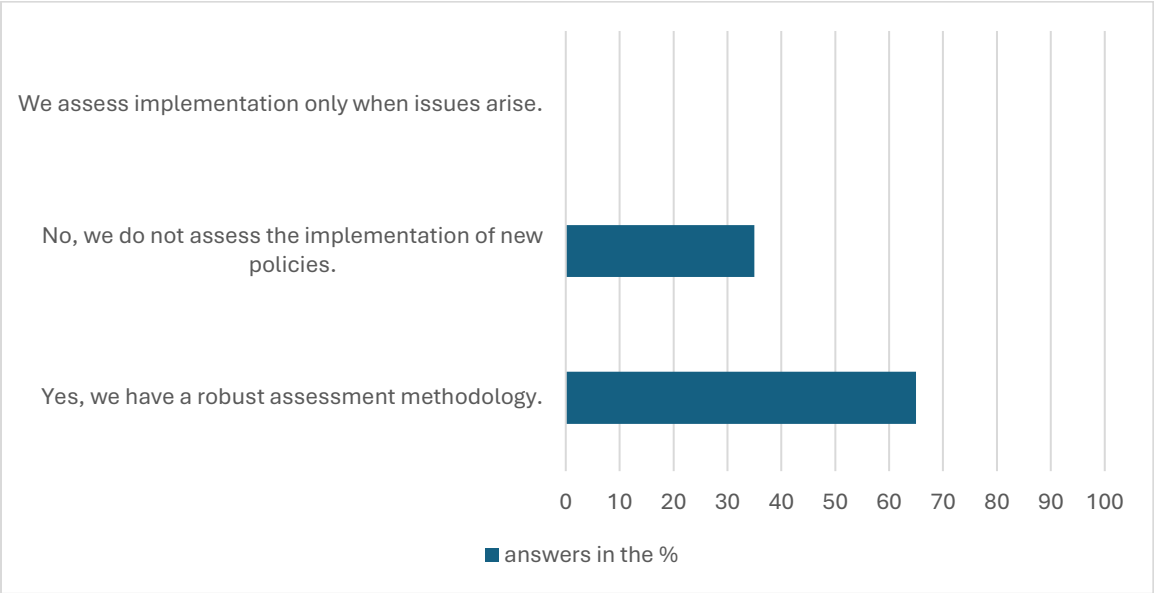
How do you ensure proper dissemination and understanding of these policies within your organization?

- ☐ Through regular training sessions and internal communications.
- ☐ By not disseminating the policies at all.



Do you have a methodology to assess the implementation of new policies and directives (National or European)?

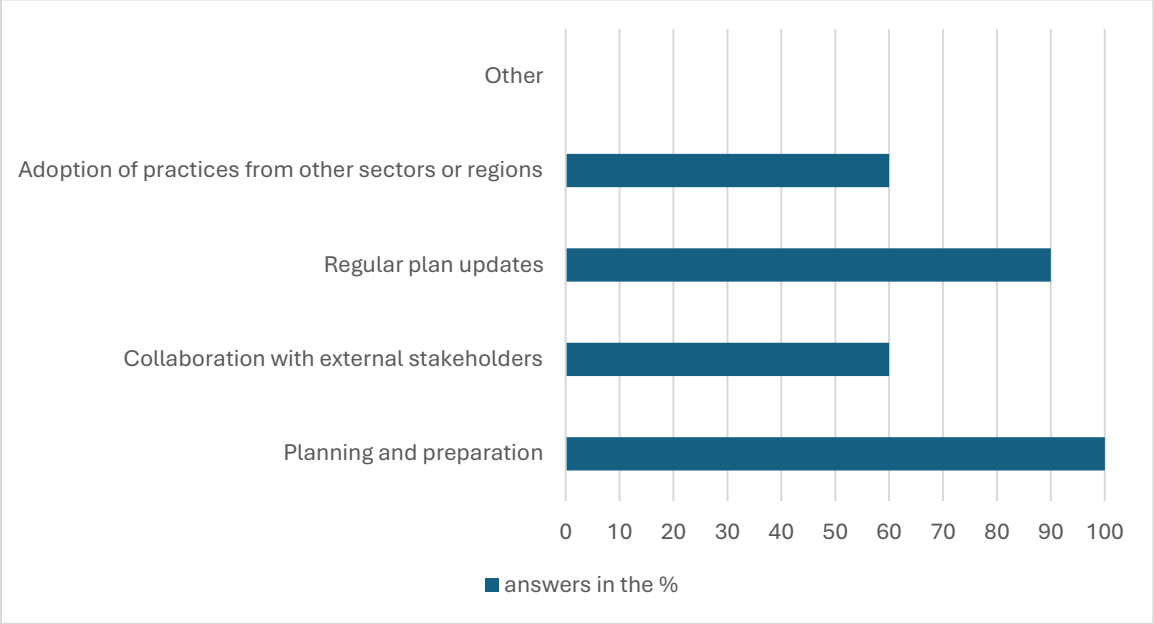
- ☐ Yes, we have a robust assessment methodology.
- ☐ No, we do not assess the implementation of new policies.
- ☐ We assess implementation only when issues arise.



What best practices in resilience has your organization adopted?

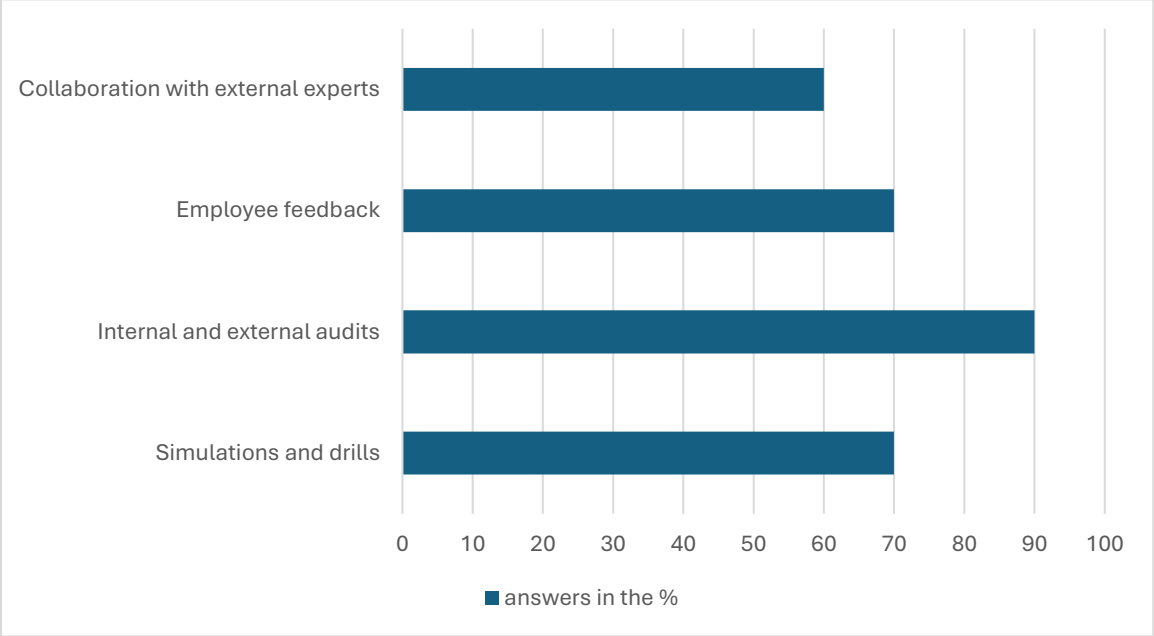
- ☐ Planning and preparation
- ☐ Collaboration with external stakeholders
- ☐ Regular plan updates

- ☐ Adoption of practices from other sectors or regions
- ☐ Other



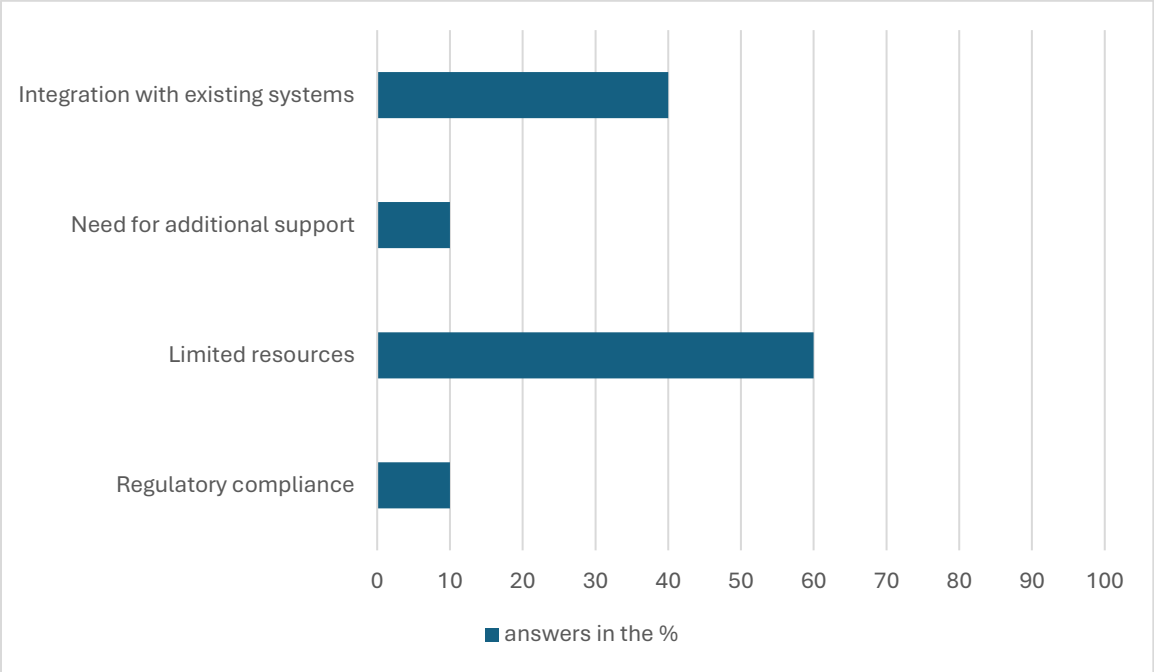
How do you test and evaluate the effectiveness of your business continuity plans?

- ☐ Simulations and drills
- ☐ Internal and external audits
- ☐ Employee feedback
- ☐ Collaboration with external experts



What challenges does your organization face in relation to new EU directives, such as NIS2 and CER?

- ☐ Regulatory compliance
- ☐ Limited resources
- ☐ Need for additional support
- ☐ Integration with existing systems



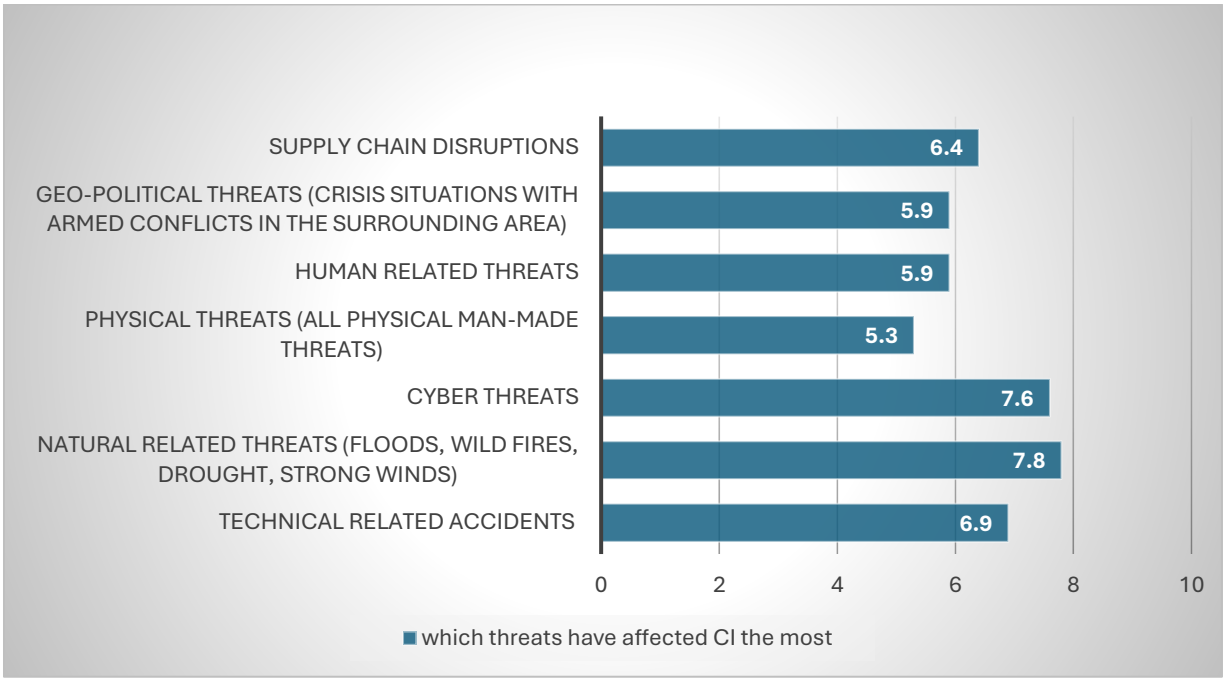
DISCUSSION PANEL 2

Suggestion for definition and concretization the most representatives use cases connected with providing resilience of CI.

Threats evaluation:

1. Please evaluate according to your experience and sector related specifics which threats are the most influenced for providing resilience of your Critical infrastructure? (Evaluate each threat with Likert scale 1-lowest influence – 10 - strongest influence

Technical related accidents	1	2	3	4	5	6	7	8	9	10
Natural related threats (floods, wildfires, drought, strong winds)	1	2	3	4	5	6	7	8	9	10
Cyber threats	1	2	3	4	5	6	7	8	9	10
Physical threats (all physical man-made threats)	1	2	3	4	5	6	7	8	9	10
Human related threats	1	2	3	4	5	6	7	8	9	10
Geo-political threats (crisis situations with armed conflicts in the surrounding area	1	2	3	4	5	6	7	8	9	10
Supply chain disruptions	1	2	3	4	5	6	7	8	9	10



2. Have you experienced a risk in the last two years following the COVID-19 period that had a very strong impact on ensuring the resilience of your organization?

If you answered YES, please state what these threats were:

Half of them responded with "YES" and listed the following set of threats:

- Threats related to electricity supply
- Floods
- Wind
- Reduction threats
- Increase in electricity costs.

3. If you had the opportunity to design a scenario for a national crisis response exercise to ensure adequate business continuity and resilience in your sector, which risk would be central to your scenario?

Name the two most exposed:

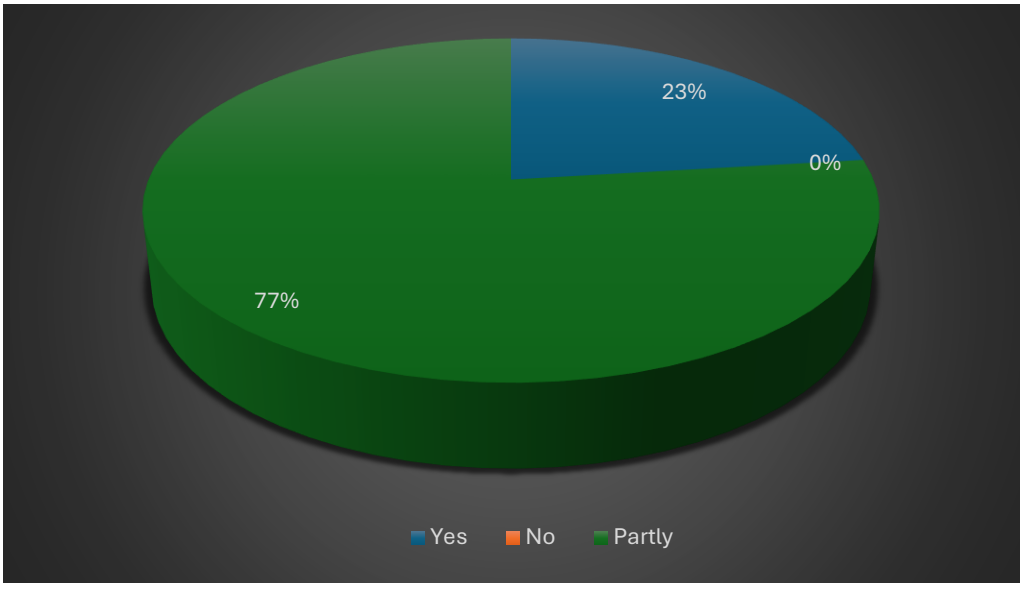
- Weather phenomena.
- Cyberattacks.
- Natural disasters (e.g., earthquakes).
- Failure of more than two elements of the power system (EES), resulting in power supply disruption.
- Communication device failure.
- Cyberattack on the SCADA energy system.
- Cyberattack on supporting infrastructure and telecommunications systems.
- Crisis response national exercise scenario depends on the threats relevant to the country. Relevant scenarios may include more than one.

- ☐ Scenario 1: In recent years, the country and neighbouring countries have been exposed to natural disasters, resulting in power supply failures, optical connection outages, and equipment outages at certain locations. Although the scenario has been tested before, it is reasonable to conduct an additional exercise. An earthquake threat can be included in the same scenario.
- ☐ Scenario 2: A large-scale cyberattack involving various types of attacks, such as malicious traffic (e.g., DoS and DDoS attacks), unauthorized traffic redirection, and illegal data interception.

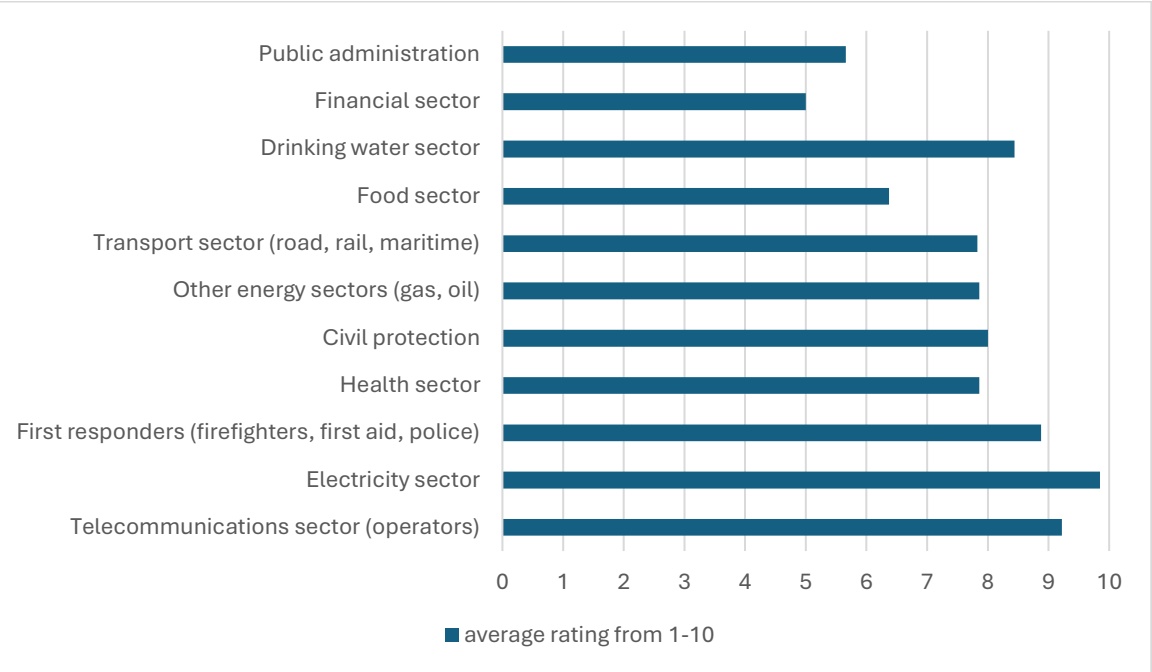
- Lack of electricity and the need for prioritized electricity supply.
- Inaccessibility of the emergency center (disruption of access routes).
- Natural disasters like floods affecting physical infrastructure.

4. Do you think that you can ensure the resilience of your sector through activities and resources within your Critical Infrastructure sector?

☐ YES
☐ No
☐ Partly



5. In your opinion, who should be even more involved in the preparation of test scenarios that would ensure an increase in the resilience of the operation of critical infrastructure and, consequently, the wider social community? (Rate on a scale of 1-10 (1- not at all-10 very important)



DISCUSSION PANEL 3

Technology related expectations with influence to stronger resilience of CI.

Current tools and their Impact:

- Which existing technology tools in your operational environment do you believe most effectively contribute to risk assessment and resilience of your CI? e.g.: Network monitoring tools, incident response systems, predictive analytics, etc.

  - **Network monitoring tools, incident response systems, predictive analytics:** These tools help detect, respond to, and predict potential disruptions, playing a crucial role in ensuring resilience.
  - **Risk assessment tools and methodologies:** These are provided by relevant ministries, and in the case of defense planning, the Ministry of Defense plays a key role.
  - **Monitoring center, tools for monitoring and detecting anomalies in the internal network:** These systems ensure proactive monitoring of network integrity and early detection of issues.
  - **Central SCADA control system and telemetry system:** They provide a high level of automation, reducing operational and human risks.
  - **Various cybersecurity systems:** These significantly lower the risks of cyberattacks and contribute to overall system resilience.
  - **Management systems:** They offer insights into risks and help shape decision-making, gradually increasing resilience by improving risk awareness.
  - **Information tools:** Essential for quickly detecting and resolving problems, these systems include network and service monitoring tools, fire detection, water, temperature control, and intrusion detection systems, video surveillance systems, and security event and incident management systems. These tools are part of the NOC (Network Operations Center).

- **Tools and systems for ensuring resilience against specific threats:**
  - **Physical security:** Fences, doors with multiple access controls before entering secured areas.
  - **Protection against power outages:** Uninterruptible power supply (UPS) systems, fixed and mobile diesel generators.
  - **Temperature control:** Air conditioning systems to prevent overheating.
  - **Equipment continuity:** Spare parts for hardware, stored software versions, backup data, and technical support contracts with suppliers.
  - **Fire safety:** Active fire suppression systems.
  - **Cybersecurity protection:** A dedicated SOC (Security Operations Center) equipped with specialized tools and staff to monitor and respond to cyber threats.

These tools and systems provide the necessary infrastructure to support resilience efforts, ensuring that critical functions are maintained and threats are effectively managed.

Assessment of technology performance:

- On a scale from 1 to 10, how would you rate the efficiency of current technology in supporting the resilience of your CI?

The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10
The effectiveness of current technology in supporting the resilience of your AI	1	2	3	4	5	6	7	8	9	10

Please explain your assessment:

1. The company has established tools, systems, and procedures, but opportunities for improvement still exist.
2. In today's interconnected world, it is essential to use advanced technologies to ensure global connectivity and manage essential services.
3. Both methodologies include the "frequency" of risk, which technically means that fire is currently assessed as a low-probability risk to our organization, as it has not occurred for a long time.
4. Current technology allows for early detection and response to threats, but better integration with advanced tools, such as AI and automation, is needed.
5. To better monitor potential threats, sensors in various systems would be required.
6. Relatively few incidents and the team's response.
7. Within the scope of capabilities, we implement the latest tested technology.
8. Existing technology requires upgrades.
9. From the perspective of elemental and technical risks, there are currently no technologies that would provide significantly higher levels of resilience. From the perspective of cyber risk resilience, the technology is sufficient to prevent serious consequences from less skilled actors.
10. Improvements and additions are certainly possible.

Future technological needs:

- **What specific types of technology advancements do you anticipate will be most crucial for enhancing the resilience of CI in the next 3-6 years?** ***e.g.: AI-driven analytics, enhanced cybersecurity protocols, advanced automation tools, etc.***

  - AI will be an integral part of all systems in the future (primarily playing a role in forecasting and adaptive actions).
  - New types of batteries for uninterruptible power supply systems.
  - Lower power consumption of equipment, thereby reducing cooling requirements.
  - Video analytics for physical security purposes.
  - Access control systems based on biometric data.
  - Artificial intelligence with optimization of cybersecurity protocols, including the human factor.
  - The methodology supported by AI will be crucial in improving risk prediction and assessment, as it will incorporate the experiences of related and interdependent organizations.
  - AI-driven analytics for improved risk forecasting.
  - Enhanced cybersecurity protocols.
  - Advanced tools for crisis response automation.
  - Advanced OT (Operational Technology).
  - Advanced cryptography.
  - New tools for ensuring physical security (automation, drones).
  - Cybersecurity combined with AI.
  - New simulation models for training.
  - Unified communication and automation of generated messages for notification.
  - Sensors in IT/OT environments.

- **For what critical information useful in the context of the project do you foresee restrictions to share outside your internal environment?**

  - The most critical information includes vulnerabilities in networks, systems, and services.
  - All documents, information, and data classified as confidential or business secrets.
  - Data about network vulnerabilities.
  - Operational continuity time (water, food, fuel, material reserves, etc.).
  - Information about vulnerabilities and security mechanisms.
  - Details about previously affected systems and corrective actions taken.
  - Plans, measures, and procedures.
  - Organization of the response.
  - Structure of process automation.

Identification of gaps:

- What major gaps or shortcomings do you currently see in the technology ecosystem and internal processes that impact the resilience of CI? (Open discussion to capture diverse insights.)

  - Upgrade of the command center and functionalities.
  - Sophisticated VOC (Cyber Operations Center) for cybersecurity.
  - A wide range of communication models for different operators.
  - Workforce.
  - Appropriate environment that connects all stakeholders in critical infrastructure (CI).
  - Insufficient training of staff to operate in critical conditions.
  - Connection of processes and activities of operators in case of major natural disasters.
  - Insufficient integration of different systems for incident response.
  - How to ensure the safe and trustworthy exchange of data and information.
  - Lack of coordination in response plans among interdependent sectors.
  - Lack of knowledge about the needs of interdependent sectors during a crisis.

User experience and expectations:

- What is your experience in multi-sector and multi-national initiatives? Please give some examples.

  Positive:

  - Participation in EU projects has enabled the exchange of best practices and improved resilience.
  - Initiative for sharing a list of essential service providers.
  - Initiative for ensuring external power supply.
  - Initiative sent to AKOS (Agency for Communication Networks and Services) regarding improvement of communication and problem resolution.
  - A good opportunity for exchanging best practices.
  - Collaboration with international associations.

- Cooperation with sectoral actors and associations.
- Connecting with neighboring countries.

Negative:

- Not the best, no involvement in planning, one-sided approach.
- We have little practical experience in this area. Most of our experience comes from collaborating with emergency services (police, firefighters, military), where we always face communication issues due to different communication systems.

- **What would be the major obstacles you would foresee in implementing new technologies and processes?**

  - High implementation costs;
  - Lack of personnel;
  - Misalignment with the company's operations;
  - Overly high investments;
  - Expert staff;
  - Time required for implementing tested systems;
  - Recognition of costs by regulators;
  - Limited resources;
  - Shifts in thinking and habits of people;
  - Financial resources;
  - Over-specialization, lack of breadth;
  - Trust in the security of technologies;
  - Financial resources;
  - Inter-sector compatibility.

- **What features or improvements would you like to see in future technological tools to better support CI resilience? e.g., better integration, user-friendly interfaces, real-time updates and warnings, federated ecosystems, pre-defined procedures/handbooks.**

  - Simpler management and maintenance;
  - Standardized interfaces;
  - Digitalization;
  - Interconnection and alerting between common stakeholders;
  - Better integration and connection of ecosystems;
  - Well-designed plans that include all stakeholders;
  - Better integration, user-friendly interfaces, real-time updates and alerts, unified; ecosystems, pre-defined procedures/manuals;
  - Inter-sector integration with extended technological capabilities;
  - Improved response in case of security incidents;
  - Reducing costs (fewer outages, fewer personnel, etc.);
  - User-friendly interfaces;
  - Technologically supported centralized crisis response management (National center for crisis management);

- Real-time updates and alerts.

4.2 Local workshop in Romania

This national workshop "Finding appropriate solutions to ensure increased resilience of critical infrastructure" aims to identify country-specific challenges, evaluate current practices, and explore improvement opportunities through practical use cases. Thus, we will tackle topics of utmost importance such as current strategies and policies for disruption management, business continuity plans, and more. The event was organized at DNSC headquarter in Bucharest and online, in 17th of December 2024, with the support of Romanian project partners: EVIDEN TECHNOLOGIES SRL, MINISTERUL SANATATII (MS), CLINICA GINECOLOGIE DR. MUNTEAN SRL, DIRECTIA GENERALA DE PROTECTIE INTERNA (DGPI).

WL1 engages and brings together experts in critical infrastructure resilience from the consortium and beyond. The workshop attracted a total of 42 participants, with 16 attending in person and 26 joining online.

The attendees represented a diverse range of sectors, including healthcare, transportation, public administration, regulatory authorities, and private enterprises.

The questionnaire included a dedicated section that allowed participants to articulate, in their own words, their industry and the related activities focused on enhancing critical infrastructure resilience within their organization.

4.2.1 Questioner results and discussion

Discussion Panel 1

Definitions of resilience

While participants agree on the broad sense of resilience – perceived as a concept covering the way you deal with crises from anticipation to management, while preserving business continuity and/or effectively restoring operations following any disruption to digital services – different institutions emphasized or introduced also more-specific points of view, as follows:

A. the recovery phase needs highlighting as it involves learning and transforming processes that allow to effectively manage future crises in a centralized manner (physical questionnaire).
B. collaboration with various institutions to research and develop advanced technologies for the protection of critical infrastructures: exchanging best practices and information on emerging cyber threats to increase incident response capacity and promote education and awareness around cybersecurity (National Institute for Research & Development in Informatics ICI Bucharest).
C. prioritize elements of preparation and simulation such as TTX (Euro-Atlantic Resilience Centre E-ARC)

D. prioritize prevention as it seems to be subpar at the national level (DNSC)

Resilience in CI operations

Resilience in different sectors can mean different things, such as:

A. risk prevention and minimization; rapid response capacity; rapid recovery; redundancy and operational continuity; ongoing assessment and improvement of systems (physical questionnaire).
B. all the elements that enable the provision of high-quality (medical or other) services, from electricity and water supply to IT and communications systems.

A consensus is reached with the conclusion that a national strategy that aligns with the European framework for resilience is required to develop sector-specific approaches to resilience.

Potential risks generated by resilience not being applied in specific sectors

Failure to properly apply the resilience principle may result in several risks and consequences, such as:

- affected operational continuity
- major financial losses
- loss of sensitive data and information
- unavailability of critical systems and processes leading to decreased productivity
- reputational damage
- adverse psychological effects
- increased recovery costs.

The risks enumerated here are common to all entities and are joined by 2 sector-specific risks, as follows:

- severe legal and financial consequences associated with data loss given the highly sensitive and confidential nature of medical records,
- legal penalties and sanctions related to regulatory compliance: Clinics are required to adhere to specific security and business continuity standards.

Resilience area: sector-specific risks and prioritization

We have classified risks into 3 main categories, later dissected as per the sector specifics: human, physical, and cyber.

The medical sector places the cyber domain at the top of the list, highlighting ransomware attacks targeting the healthcare sector and patient data breaches.

The human domain poses a medium to high-priority risk, with key threats such as data breaches leading to privacy breaches and potential legal consequences, credentials theft, theft of medical supplies and medical equipment or processes sabotage compromising patient safety.

Finally, the physical domain poses a medium to low-priority risk, with threats such as biological risks and motion risks caused by physical strain.

Moving away from the medical sector brings additional risk classifications to the table, such as: risks stemming from technological failures and human errors as well as social, political, and economic risks.

Still, cyber risks are deemed among the most critical, as attacks of this nature can severely disrupt the operations of critical infrastructures.

Prioritization changes slightly in ICI's vision with physical risks being placed right after cyber-associated threats due to their immediate impact, often resulting in long-term disruptions.

Finally, we have the risks associated with equipment, software, or hardware failures that can significantly impact system performance despite being relatively common and manageable.

The last two types of risk can have a devastating long-term impact and lead to overall instability.

Main policies and directives related to organizational resilience

The consensus implies that several types of regulations apply, depending on the sector. Thus, we can have operations-specific legislation, compliance with internal mechanisms for building and consolidating resilience such as institutional policies and regulations at the local level. Then, there is the national level with associated including legislation on civil protection, public health, and cybersecurity and finally, the international level characterized by mechanisms such as the Directive (EU) 2022/2556 and Regulation (EU) 2022/2371.

In addition, the Clinic representatives also mentioned organization-specific standards such as ISO 27799:2016 and ISO 31000:2018, ISO 22301:2019, ISO/IEC 27001:2013.

Regulating authorities related to organizational resilience

Among the mentioned entities, we enumerate:

- Ministry of Health
- National Institute of Public Health
- Directorate of Public Health (regional and county level)
- World Health Organization (WHO)
- European Commission
- ENISA (European Union Agency for Cybersecurity)
- ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

Organizational standards and their status (mandatory, optional)

ISO Standards (ISO 31000:2018, ISO 22301:2019, ISO/IEC 27001:2013, ISO 27799:2016)

Internal and/or external audits related to compliance with standards or directives

The sole respondent (medical clinic) mentions that their organization conducts the following audits to ensure compliance with ISO standards:

Internal audits: These are conducted annually and involve documentation review, staff interviews, and process observations to identify non-conformities and areas for improvement (updates to policies and procedures, data protection measures, incident response protocols, and medical staff training).

External audits performed every three years: Supplemented by annual surveillance audits to uphold certification, these audits focus on internal process optimization, resilience against natural disasters and pandemics, and effective risk management through incident reporting and medical resource management. They help identify deviations from standards, opportunities for improvement, and best practices.

Formally approved guidelines or procedures to supplement standards

The sole respondent (medical clinic) mentions that their written procedures detail comprehensive policies for risk management (and operational continuity), data protection, and emergency preparedness (incident response procedures) and are complemented by regular internal audits and staff training (best practices).

Methods to integrate resilience into sector's strategy or operations

The consensus on this topic is that integration is realized through regular risk assessments and mitigation strategies.

Internal policies to implement new directives and regulations on resilience

The consensus on this topic is that the different organizations possess internal policies allowing them to implement new directives and regulations on resilience.

Authorized procedures and dedicated teams responsible for resilience efforts

The consensus on this topic is that the different organizations have authorized procedures and dedicated teams responsible for resilience efforts.

Dissemination efforts related to organizational resilience policies

The prevailing agreement on this topic is that initiatives for resilience dissemination are implemented through regular training sessions and internal communications.

Assessment methodology related to implementation of new policies/directives

While most organizations reported having strong assessment mechanisms in place, there is a lack of consensus on this issue. One respondent noted that their organization does not engage in assessment activities related to the implementation of new policies.

Best practices in resilience at the organizational level

The consensus on this topic emphasizes that effective planning, preparation, and collaboration with external stakeholders are critical best practices for organizational resilience. However, opinions diverge regarding the necessity of regular plan updates. Two respondents view these updates as essential, while a third respondent advocates for incorporating practices from other sectors and regions to enhance the overall framework of resilience best practices.

Testing and evaluation effectiveness of business continuity plans

1. A: Simulations and drills, collaboration with external experts
2. B: Simulations and drills, internal and external audits, employee feedback
3. C: internal and external audits

Organizational challenges in relation to new EU directives (NIS2, CER)

Answers include mentions of limited resources and emphasize the need for additional support.

Discussion Panel 2

Most influential threats to resilience in specific sectors

We have used a 1-10 scoring system to rate the threats. Out of these results, we selected the top 3 mentions having obtained the highest grade (closest to 10).

As such, geo-political threats, cyber threats, and supply chain disruptions occupy the first 3 positions in the rank, with associated grades ranging from 7 to 10.

Additional comments regarding this risk trinity include AI (AI intervention in decision-making, drones, emerging technologies, or obsolete technologies.

Additional risks having made it to top 3 include malicious use of technology by user, physical threats, and technical accidents.

Post-COVID organizational risks with a strong impact on resilience

Answers include mentions of massive staff fluctuation, cyber-attacks, and consecutive DDoS attacks.

One answer refers to effects of the previous pandemic with a direct impact on the population and communities and encourages intensive analysis to help prepare for similar events in the future.

High-importance risks to consider when designing scenarios for national crisis response exercises

A: interconnections between systems and domains, which often reveal gaps or overlaps (unclear responsibilities or overlapping competencies, resulting in participants or stakeholders assuming that someone else will address the issues at hand)

B: overlapping of two or more threats

C: Distributed cyberattack on multiple infrastructures and Physical damage to telecommunications networks over a wide area (such as an entire city, for example)

D: Cybersecurity threats, including potential ransomware attacks, could disrupt critical healthcare services, compromise patient data, and disrupt communication systems.

Such incidents can have an immediate and widespread impact on the clinic's operations, affecting all aspects of the organization, from patient care to administrative processes.

Supply chain disruptions: During a crisis, such as a natural disaster or pandemic, the supply chain for essential medical supplies, drugs, and equipment can be severely disrupted. This can lead to shortages, delayed treatments, and compromised patient care, highlighting the need for robust supply chain management and contingency planning.

Resource sufficiency to ensure resilience at the CI sector level

Of the four respondents who provided feedback regarding this inquiry, two indicated that they believe the sectoral resources are adequate to ensure the resilience of their critical infrastructure. The other two respondents expressed that the current resources are only partially sufficient.

Sector involvement in developing test scenarios related to resilience

We have used a 1-10 scoring system to rate the threats. Out of these results, we selected the top 3 mentions having obtained the highest grade (closest to 10).

A: single domain testing is insufficient - It is essential to evaluate multiple domains under extreme scenarios that rapidly approach a critical threshold. Beyond this point, the focus shifts from individual domains to the overall integrity of the entire system.

B: Public administration (local and central) should be more involved and participate actively in developing drills in cross-sector domains (using tools like Poseidon for exercise implementation). For instance, the E-ARC Red Cell could help:

- identify critical thresholds that may lead to system failure,
- develop collaborative solutions for coordinated exercises involving all stakeholders,
- develop annual strategic plans,
- activate mechanisms at the European level, as applicable.

C: rated entities with 1-10 scale, top 3 picked here: civil protection – 10, public administration – 9, drinking water supply sector – 8

D: public administration – 9, telecommunications sector – 8, civil protection – 7

E: electric power sector - 8, public administration and first responders – 7

Discussion Panel 3

Existing technology tools contributing to risk assessment and CI resilience

• DG ARC has conducted research on the interdependencies among key areas critical to EU resilience, utilizing indicators to assess cross-sectoral impacts and to explore future development directions.

• Hybrid solutions – air quality in Smart Cities. The platform is useful, but it should work distinctly and in real-time; federalization agreements versus GDPR

• Network monitoring tools, firewall, antivirus, VPN for remote connections, automatic monitoring and alerting systems, regression testing, periodic penetration testing of critical applications conducted with an external company, IP-based access restriction for critical systems, etc.

• VPN for encrypted connections, UPS for increased resilience (power source for critical equipment, in case of power outages), alarm system with security company contacts (real-time monitoring and alerting, supplemented by security teams' interventions to investigate potential dangers on-premise).

Efficiency of current technology in supporting CI resilience

We have used a 1-10 scoring system to rate the threats. Out of these results, we selected the top 3 mentions having obtained the highest grade (closest to 10).

A: The platform must receive the results and then update them accordingly. Centralized elements/information must be made available (radio, TV, mass- media sources).

B: rate 9, The existing technology supports the resilience of our systems.

C: rate 8 + explanation below

Existing tools provide robust protection against cybersecurity threats, ensure continuous power supply during outages, and enhance physical security. However, there is always room for improvement with additional integrations: real-time alerting and coordination with other healthcare entities, automatic firmware updates, interactive training on cybersecurity awareness for healthcare staff, advancements in surveillance with HD video cameras, advanced inventory management software to track medical supplies and equipment for timely replenishment, advanced backup systems.

Anticipated technological advancements (3-6 years) to enhance sectoral CI resilience

A: Early warning systems boosted by future technological developments, controlled by and with human supervision.

B: The platform could also integrate the crisis management component; Medical prevention based on sensors in the smart watch.

C: Over the next 3 to 6 years, technological advancements will play an essential role in strengthening the resilience of critical infrastructure and ensuring an effective response to emerging risks. Some of the most important advances in the field include artificial intelligence and machine learning; IoT and

advanced sensors; Blockchain; Cloud Computing, Virtual Reality; 5G and advanced telecommunications networks; and cutting-edge cybersecurity technologies.

D: Respondent provides a 4-point list available below:

- Cloud-based security: allows a secure and scalable way to store data backups, as well as other benefits such as data encryption, two-step/multifactor authentication, and detection of possible breaches.
- Artificial Intelligence: detect anomalies using Machine Learning to analyze large amounts of data over a short period and automate responses to various incidents.
- Blockchain: Help secure data and manage identities.
- Secure IoT: connect medical devices for safe operation and secure the data generated by these medical devices.

Critical project information with potential sharing restrictions to external environment

A: indicators reflecting the normal functioning of a system, and more importantly, the limits (thresholds) that, when exceeded, signal high attention, potentially indicating a pre-crisis or even crisis.

B: Confidential patient health information; specifications regarding network configurations, security protocols, and incident response strategies; data on healthcare providers.

Major gaps in the technology ecosystem & internal processes impacting CI resilience

A: Siloed work and lack of an integrated institutional image

B: Insufficient staff training on cybersecurity protocols in some organizations and access to internal systems without a VPN.

C: Cybersecurity vulnerabilities, Outdated technology that cannot withstand modern threats in the medical field, Interoperability issues, and Insufficient staff training.

Experience with multi-sector and multi-national initiatives

Collaborating with NGOs and international organizations can facilitate the development of community health programs targeting specific health issues, such as those supported by the Global Fund to Fight Disease. Engaging in partnerships with the European Public Health Alliance (EPHA) can greatly enhance public health systems and strengthen the overall healthcare infrastructure by tackling various health policy issues and promoting improved health standards and practices throughout Europe.

Major obstacles in implementing new technologies and processes

- Financial constraints: Limited budgets make it difficult to invest in advanced technologies and necessary infrastructure.
- Lack of technical expertise: Hiring new experts can be costly and time-consuming.
- Resistance to change: Staff may be reluctant to adopt new technologies due to familiarity with existing systems or fear of the unknown.

- Interoperability challenges: Integrating new technologies with existing systems can be difficult due to the lack of standardized protocols.

Features & improvements to be included in future CI resilience-focused technology tools

- Better integration: Future technology tools should be able to easily connect to electronic health records, laboratory systems, and other healthcare applications.
- User-friendly interfaces: Technology tools with intuitive, easy-to-use interfaces can increase productivity, reduce errors, and help reduce learning time for healthcare staff, which is especially important in busy clinical environments.
- Real-time updates and alerts: Tools that provide real-time updates and alerts can help clinics respond quickly to emergencies and changing situations.

4.2.2 Conclusion

Discussion Panel 1

1. Defining resilience

In addition to conventional definitions, key concepts such as preparation and simulation are emphasized in relation to resilience.

However, high costs and production disruptions are significant obstacles. E-ARC has proposed a structured approach focused on cross-domain and cross-sectoral tabletop exercises, supported by central administration. The main takeaway is that legislative backing and sufficient resources are essential to facilitate progress and enhance collective resilience.

2. Resilience in critical infrastructure operations

The focus is on collaboration, with institutions recognizing resilience as a collective responsibility that extends beyond individual sectors.

A national framework is essential to effectively developing sector-specific resilience strategies. Therefore, the government should take the lead in managing this initiative. A top-down approach is crucial, with the government spearheading the effort and executing a comprehensive action plan.

Discussion Panel 2

1. Threat evaluation

The main risk factors are associated with cyber-attacks, frequently executed by activist groups and they encompass a wide range of threats, including DDoS attacks, deepfakes, and hybrid campaigns. Geopolitical threats, particularly from state actors with significant resources, are also a critical concern, as they can disrupt supply chains and are typically ranked just below cyber threats in terms of importance. Additionally, emerging and outdated technologies are considered pressing risks that must be prioritized to enhance resilience.

2. **Involvement in resilience-related test scenarios preparation**

The emphasis is once again on strategic collaboration among cross-sector organizations and authorities to develop and define interactive scenarios. This approach should enable live testing to demonstrate preparedness, identify vulnerabilities, and uncover opportunities for improvement.

Consequently, the focus shifts to training spanning multiple domains rather than operating in silos and highlighting the intersections where competencies overlap.

Discussion Panel 3

1. **Technology tools shaping CI resilience**

A distributed (or hybrid) platform guarantees operational continuity. Additional features focus on

integrating situation management capabilities to facilitate simulations.

Data can be collected from various sources, including institutions, or individual users of the platform wearing devices such as smartwatches with a range of sensors that track daily activities. This data must be depersonalized to ensure efficient use and to safeguard confidentiality.

Finally, the platform should connect 112 with ISU to streamline communication and avoid repetition. This represents a forward-looking project aimed at enhancing operational efficiency in emergency response.

Final Summary

Tools:

- Development of socio-mathematical models that address resilience (Black Swan) to assess social responses and community health.
- Establishment of a Resilience Scoring Standard.
- Management of emergencies through the platform.

Procedures and Processes:

- Formulation of "Imperative Procedures" for effective resilience management.
- Creation of a national resilience strategy, including sector-specific legislation.
- AI Directive/ European legislation to guide the ethical use of artificial intelligence.
- Establishment of minimum resilience requirements.
- Budget and resource allocation
- Post-crisis evaluations to derive lessons learned.

Organization:

- Implement predefined crisis management structures, with clearly defined roles and responsibilities in resilience and crisis management (establish ISU working groups).

- Address ISU civil protection issues.

Threats:

- Geopolitical risks.
- Ethical considerations surrounding Artificial Intelligence:
  - Development of AI ethics legislation.
  - Regulation of accepted AI models.
  - Continuous monitoring of AI models.
- Challenges posed by emerging and/or obsolete technologies.
- Waste management issues.

4.3 Local workshop in Italy

The first Italian workshop was held on 28th of November 2024, in INSIEL headquarters in Trieste, Italy. It was led by INSIEL (INS) as Italian micro-pilot leader. The organizations involved to discuss on all aspects around “essential services” and “resilience” were Insiel, as ICT providers for Public Administrations and the Friuli Venezia Giulia Region, as public authority that defines and finances all digital information system at regional level, including connectivity infrastructure, data management infrastructure and software, cross-domains, used by public administrations with Friuli Venezia Giulia Region.

The total number of participants was 18, composed by 2 facilitators (employees from INS), 5 participants from Friuli Venezia Giulia Region and 11 participants from Insiel.

The participants hold management positions in the following areas:

- Cybersecurity
- Privacy
- Data Center
- Telecommunication projects & services
- Innovation and ICT governance
- Regional Broadband
- Information System, digitalization, and e-government

The adopted methodology for the local workshop includes a set of discussion panels. Three surveys have been prepared in advance and distributed to all participants during the workshop, in order to trigger an open discussion and maintaining the focus on ENDURANCE topics.

As planned in the agenda, the workshop started with an overview presentation of ENDURANCE project, followed by the planned discussion panels, supported by dedicated surveys.

4.3.1 Discussion Pannels

Discussion Panel 1 and 2

The objective of Discussion Panels 1 and 2, underpinned by Survey 1, is to gain a deep understanding of the concept of resilience across different areas including digital services within Public Administrations.

To begin with, it is noteworthy to highlight that the longest and most engaging discussion centered around the concept of resilience. A key takeaway is that the interpretation of resilience varies according to the specific working context. While the main definition common to all departments focuses on ensuring business continuity, the discussion also brought forth other perspectives on the concept of resilience. Resilience is:

1) When an organization is able to proceed in presence pf a strong change. In this case the focus is on how the organization react in case of a change. This change can be planned, for example a patch to a software, or unplanned due to human error in implementing an upgrade of a software.
2) When an organization is able to solve a problem. From a Public sector perspective, the resilience can be the capacity to communicate to citizens an interruption of public services; a prompt and a proper communication can be a way to be resilient.
3) When an organization is able to predict an event that is a risk for the business continuity. The security index, in particular in the cybersecurity and privacy domain, is composed of the following phases: prevent, react, recovery. In this perspective resilience is measured bases on the time it takes for the organization to return to normal. Of course, the measurement of the resilience, based on time to go back to the normality, is different from type of services and type of systems.

Moreover, from the discussion about resilience, the risk management raised out as a crucial part of an organization. In case of certainty of the risk, an organization can define itself as resilient if it is able to reduce the impacts of the risk. The types of risk are operational, economic and reputational. In some area of public health, the risk of an error in the management of information systems can lead to physical harm to people, such as the management of bar codes in the transfusion sector.

An interesting concept has been raised during the discussion, it is the NO-RESILIENCE, it is an unknown status, totally out of the organization awareness.

Concerning the type of risks that can affect the resilience of Public Administration and its Digital sector they are cyber, physical and human, having same priority.

Concerning the **legal framework** for the Italian micro-pilot, we can mention:

- National Cybersecurity Law n.90/2024.
- Guideline of ACN (National Agency for Cybersecurity)
- NIS2
- CER directive
- CRA – Cyber Resilient Act

- GDPR

Concerning the **standards f**or the Italian micro-pilot, they are:

- ISO 27001
- ISO 22301
- ISO 9001
- ANSI/TIA-942 is a standard to certify Data Center. TIA means Telecommunications Industry Association, that is accredited by ANSI (American National Standards Institute).

In the particular case of the Italian micro-pilot, legal framework and standards are applied to the Digital sector of the Public Administrations by Insiel that works to be compliance with laws and to obtain all needed certification. For this reason, Insiel has its own department called "Certifications and Processes" that works in cooperation with all other departments to ensure compliance with legal framework and standards.

MODUS OPERANDI

Concerning how the digital sector of the Public Administration acts to ensure resilience, it consists in an integrated regular risk assessment and mitigation strategies, with the support of external consultants.

Comprehensive internal policies enable the organizations to implement new directive and regulations, by a dedicated team. Moreover, the internal communication and training sessions are key factors to ensure concrete resilience.

The current focus is on developing a robust methodology to assess the implementation of new policies and directives. This initiative will require time and the reorganization of certain CI processes to ensure effective execution.

The main **best practices** adopted in Italian micro-pilot are:

- Planning and preparation (relevant too)
- Collaboration with external stakeholders (it is considered a good practice)
- Regular plan updates: for example, the plan to be adopted when there is a change in the infrastructure (at HW or SW level).

The business continuity is, regularly, tested by:

- Simulations and drills (internal)
- Internal and external audits YES
- Collaboration with external experts (consultant on demand)

A common opinion, both at governance and operational perspective, represented by FVG Region and Insiel respectively, the main challenges in implementing new EU directives are the limited resources and the integration within the existing environment.

Discussion Panel 3 and 4

Supported by Survey 2 and 3

Survey 2:

Concerning the type of threats that could have an impact on CIs with related departments within the Italian pilot, the score is between 5 and 9. The lowest is related to Geo-political threats and the highest is related to cyber and human threats.

Any particular risk has occurred after COVID-19 period.

The main interesting scenarios for Italian pilot are Data Breach and Data Leak and Denial of Services.

Another point is about the level of autonomy of the CI to ensure resilience, the answer is the CI is partially autonomous.

The topic on which is the most important sector in ensuring increasing resilience of CIs, all participants agree that all mentioned sectors have 10 as score.

Survey 3

PRESENT

The discussion on technologies and their role in raising and ensuring resilience of CIs in front of threats and risks, that are constantly variable, carry out different answers and opinions that are strongly connected with the specific operational departments of the organization.

From a cybersecurity perspective the relevant tools that could contribute to risk assessment and resilience are:

- Intrusion Detection and Prevention System, SIEM, MISP.
- Vulnerability Assessment and Penetration Testing
- Security Information and Event Management (SIEM)

From an operational perspective (Data Center) the relevant tools are both the specific architectural design implemented and the usage of devices and components that have features of behavior analysis, based on predictive algorithms.

There is a growing need for networking and AI tools.

The assessment of current technologies yields a score of 7-8, indicating a good level of satisfaction with the existing tools. However, we identified areas for improvement, particularly in user proficiency through additional training. Furthermore, there is a necessity to adopt and integrate new technologies to stay competitive. In conclusion, on one side, we have the need to better understand how to implement existing technologies (training need) and on the other side, the need to adopt new technologies.

FUTURE

The needs for the future are mainly focused on AI, in order to have AI-driven analytics, predictive tools. Another line of needs is on real-time detection (thanks to AI), orchestration, advanced automation tools and training platform for cybersecurity analysts.

Concerning data sharing, Insiel needs to conduct a check for each single type of data, in accordance with GDPR and confidentiality requirements. Moreover, Insiel holds ownership of certain datasets and retains the authority to decide how and what data may be shared (in some cases some synthetics data could be needed). In other cases, Insiel acts as the Data Processor, thus it is important to obtain approval from the FVG Region for any data sharing initiatives managed by Insiel.

GAPS:

- Knowledge transfer (working in silos)
- Potential weakness in the exposition of the perimeter
- Communication between entities (also internal)
- Lack of a complete picture (fragmented knowledge and operability)
- theoretical aspects and technologies implementation tailor-made
- Additional training
- Human factors: overwhelmed workers in relation with new resilience needs. (Resource TIME)

EXPERIENCE and EXPECTATIONS

INSIEL has already experienced EU cooperation (SUNRISE, CEDAR, PIXEL, etc.). In particular, in SUNRISE Insiel with the Healthcare department of the FVG Region is testing innovative solution of cybersecurity with a focus of risks linked to a pandemic period.

From a Data Center perspective, it is essential for all components to be allocated to either a testing or production environment. Consequently, the Data Center plays a pivotal role in all activities, including the design of IT service architectures, the management of emerging technologies, and collaboration with Network and Security teams.

Concerning the main obstacles in implementing news technologies within the internal processes, a set of areas have been highlighted:

- GDPR and privacy issues – the data sharing procedures and restrictions due to privacy policies that slowed down the training of the Machine Learning algorithms.
- Lack of a common strategy between internal departments, diversity of priority linked to specific task.
- The level with acceptance and commitment with the change of processes.
- Limited resources, such as economic, human and lack of awareness of the risks deriving from not implementing new solutions and processes.

Expectation from the future:

Technological perspective:

- Real time updates and warning, integration with tools like MISP, Maltego, Shodan and other technologies for the cybersecurity realm, handbooks that will improve the response activities of our cybersecurity specialists. Adversarial Emulation plan with mitigation hints to increase the defense capabilities in the weakest points of our infrastructure.
- Technologies that are user friendly, easy to use and to integrate.

Methodological perspective: the public administration should create a dedicate team competent and able to respond quickly to new challenges.

Discussion Panel 5

Both Insiel and FVG Region will participate to the working group and will identify expert that could give additional value to ENDURANCE work, covering other sectors and providing new perspective of resilience.

4.4 Local workshop in Greece

The first Greek Workshop was organized on the 19th of December 2024 at the premises of SYNELIXIS in Athens, Greece, with remote participation of attendants outside of Athens. It aimed to bring together practitioners from different sections (Critical infrastructure operators, regulatory/oversight authorities, technology providers/enablers, and academia) to facilitate open discussion.

The Workshop was attended by a total of 11 participants from SYNELIXIS, EYDAP, RDFW, and ICCS, bringing expertise from regional authorities primarily responsible for civil protection, a CI operator, research expertise in the area of CI resilience, and technical project coordination.

4.4.1 Discussion Pannels

The workshop was structured around four panels, three of which were guided by surveys/questionnaires that had been distributed beforehand among the participants. While the purpose of the questionnaires was to help keep the discussion relevant to ENDURANCE topics of interest, there were situations where the participants felt they lacked the expertise to answer the questions. Also, a large part of the discussion during the last panel was spent brainstorming solutions related to logistics/organizational risks.

The last panel served as a forum for CI operators and oversight authorities to provide proposals/feedback and brainstorm ways to achieve the engagement of additional stakeholders. Even though the Greek micro-pilot focuses only on two sectors as defined by the CER directive (Drinking &

Wastewater Management), the workshop aimed to take a look at the broader picture and examine relations and dangers in relation to other sectors.

Discussion Panel 1: Input from CI stakeholders

The main goal of the first Discussion Panel was to gather Input from the CI stakeholders regarding their broader views of resilience and what it means, how the need for resilience affects day-to-day operations and planning, legal & regulatory framework, and lastly, responsibilities & oversight.

While the participants generally shared similar views on the definition of resilience, it was immediately agreed that the general expertise of the cohort was skewed towards an engineering point of view and focused on the ability to handle disruptions (caused by either failures or external events like floods or cyberattacks). Unfortunately, due to a lack of expertise in the area, there was little input regarding day-to-day operations & planning. As part of the participants' assessments of the importance of risks, physical risks (extreme weather, failures, earthquakes) were seen as the highest priority, with the human domain coming second and the cyber domain last due to a large part of the infrastructure (pipes/ sewers, water cleaning having no cyber-related threats affecting them).

It was clear from the discussion that due to the nature of the sector, the definition of disruption resilience skewed towards the ability to tolerate catastrophic events (e.g., the ability of the water sewage system to withstand flooding conditions, the ability to avoid adverse effects from natural disasters like wildfires or earthquakes to the quality of drinking water).

The regulatory framework affecting the Greek micro-pilot consists of all the standards/regulations around security/data protection/CI protection (GDPR, CER, NIS2, ISO 27001) and sector-specific regulations related to drinking water quality (local regulations that implement EU directives) and certification of the labs verifying the quality (ISO EN 17025).

Lastly, the responsibilities are split between CI operators (companies that handle the infrastructure), Regional Authorities (incident response/civil protection), and National Authorities (regulation, alignment to EU directives). It was identified that while in the Region of Attica, both the Regional Authority & EYDAP, who is the operator of the infrastructure, participate in ENDURANCE. At the same time, in the Region of West Greece, only the regional authority is part of the project.

Discussion Panel 2: Representative Disruption Use Cases

During the second Panel, the discussion revolved around potential disruption scenarios, risk assessment, ability to respond & dependence on other sectors, past events & lessons learned.

In accordance with what was found during discussion Panel 1, natural-related threats (all forms of extreme weather, wildfires, and earthquakes) are by far the most critical risk for the sectors involved in the Greek micro-Pilot. Extreme weather & wildfires are increasing in frequency in Greece, and earthquake threat is always present. Events like that can also have the potential for larger-scale disruptions compared to failure in a water cleaning facility that can be mitigated partially. Similarly, human risk factors were also seen as intermediate threats due to their limited impact.

Geo-political threats & supply chain disruptions were seen as emerging risks, although their potential impact is unknown. Due to the low digitization of certain aspects, cybersecurity was seen as a lower risk.

While no events that have happened recently have created large-scale disruptions in Drinking & Wastewater Management, as mentioned above, extreme weather events & wildfires are increasingly common.

As for dependence on other sectors, Power (electrical & other forms) and Telecommunications were seen as the most important. Also, due to the scale of the events with the potential to cause disruptions, the first responders were also seen as critical. According to participants who experienced the last earthquake on a scale sufficient to cause massive disruptions, Telecommunications was the sector that had the most problems and that could pose a danger in response coordination.

Unfortunately, the consensus among the participants was that while cross-sector response drills would be helpful, the logistics are beyond the participants' means because several sectors would require national and not regional participation.

Discussion Panel 3: Technology: Current State & Future Expectations

The purpose of the third Panel was to survey the current use of technology for disruption resilience and to gather input about gaps and future needs. This input can be crucial in aligning the development scheduled in ENDURANCE and guiding the work planned in Work Packages 3-8.

The main technological challenge is the lack of digitalization, with a lot of systems operating without remote monitoring. Also, the compartmentalization of data is seen as a challenge to achieving a broader picture of needs/wants. One crucial area is identifying all relevant data sets that can help risk assessment & incident response. Navigating the existing processes for accessing available information is particularly challenging due to data silos.

Generally, future technological needs revolve mainly around process improvements. In that sense, ease of use is a concern, especially when convincing departments to provide data to new systems or adopt new solutions.

Discussion Panel 4: Proposals from CI stakeholders

The purpose of the last Panel was to facilitate proposals from the CI stakeholders. The lack of personnel, budget, skill gaps, and fragmentation of responsibilities between organizations were seen as problems for all participants. One suggestion that was taken as an action point from the pilot leader (SYNELIXIS) was to prepare an initial vision of tools/services planned for development in ENDURANCE and present ways they can help specific needs of EYDAP/regions, for example, due to the catastrophic nature of some events that threaten the Drinking and Wastewater Management resilience, it is hard to predict the impact beforehand. One idea is to use simulation and advanced models to estimate it.

Also, a big part of the discussion was geared toward addressing the realization that the participants lacked expertise in the business continuity aspect of resilience.

One key opportunity that was identified was the possibility of championing a more holistic approach towards disruption resilience, raising awareness of the impact that cross-sector/supply management/cyber-related threats can have on daily operations.

Another key takeaway from the discussion panels was that overall logistics and coordination with departments not directly involved with ENDURANCE are the main challenges currently affecting the team. For example, access to historical/real-time related to drinking water quality is not public, and it might require navigating permissions/approvals. As part of a mitigation plan for the risk, the participants agreed to pursue a set of next steps that felt could help in this direction.

Here is a bullet list of what was decided:

- EYDAP/Regions to distribute the questionnaires internally to departments not directly involved in the project but can be affected by disruptions or are gatekeepers of useful data. That can help the team identify additional opportunities for impact.
- Network with departments/colleagues that might have an interest in ENDURANCE. That can help with the Working Group and also provide the team with insights.
- SYNELIXIS, as the Greek micro-Pilot leader, will prepare a presentation of use cases to showcase benefits from ENDURANCE outcomes that can be used as a sales pitch to other departments or authorities.

4.5 European workshop

The EU workshop enabled a multifaceted approach to presenting the key highlights addressed by the ENDURANCE project. In the first phase, the introductory part of the European workshop provided an appropriate presentation of the project's key steps and objectives. The main highlights from the implementation of national workshops across four countries—Greece, Italy, Romania, and Slovenia—were presented, alongside the establishment of corresponding pilot environments. Additionally, a presentation of the EU-CIP partner project was conducted, showcasing ENDURANCE's significant contribution to the repository of best practice examples in the field of critical infrastructure protection.

Besides introducing the initial steps for further discussion in later roundtable sessions, the first part also served as a fundamental briefing for the members of the Pan-European Working Group on Disruption Resilience.

In the second part of the EU workshop, the focus was entirely on opening a discussion about key aspects of ensuring the resilience of critical infrastructure. An in-depth discussion took place within the framework of four roundtable sessions. However, due to an insufficient number of participants registering for the roundtable dedicated to risk assessment, the organizers decided to postpone this topic and feature it as one of the leading discussions at the next EU workshop.

The previous section of the report provides a detailed overview of the discussion topics, summaries, and recommendations for the next steps related to strengthening critical infrastructure resilience. All inputs gathered will also play a significant role in drafting the European strategy for critical infrastructure resilience.

The detail report fork EU workshop is attached in ANEX-2 of this deliverable. In the following section, we will outline some of the broadest conclusions from the discussion. All details are available in the recorded discussions from each roundtable session.

1. Purpose and Vision of the ENDURANCE Project

- The project aims to enhance strategic cooperation and create a pan-European platform for resilience coordination.
- Its focus is on exchanging best practices, knowledge, and experiences related to the resilience of critical services.
- One of its primary goals is to support EU Member States in implementing legal frameworks such as the NIS Directive, CER Directive, and others.
- The project includes 12 national workshops and 3 EU-level events, with this being one of the first.

2. Structure of the Workshop

- The session began with three key presentations, followed by a division into five virtual roundtables, each focused on a distinct theme.
- Participants were invited to engage in honest, in-depth discussion on challenges, lessons learned, and practical experiences.
- The roundtables were designed to foster idea generation, identify gaps, and produce actionable insights for resilience-building.

3. Harmonization of Legal and Strategic Frameworks

- A core topic was the need to harmonize national approaches to resilience with existing EU directives.
- Participants discussed the challenges of transposing EU-level documents into national legislation, and how alignment remains uneven.
- The goal is to streamline understanding and implementation across sectors and countries for more effective coordination.

4. Strategic Communication and Coordination

- The session underlined the importance of strategic-level coordination across public and private entities.
- Effective resilience planning was said to rely on continuous, structured communication, not only during crises.
- Roundtable discussions emphasized the value of mutual support and information-sharing before, during, and after disruptive events.

5. Sectoral Implementation Challenges

- Participants shared challenges in adapting resilience frameworks to different sectors (e.g. energy, water, transport, digital).
- The group acknowledged that sector-specific needs must be balanced with unified EU guidance.
- Discussions covered gaps in technical resources, knowledge, and the operationalization of policy into practice.

6. Roundtable-Based Knowledge Exchange

- Each breakout session produced practical input on key topics such as resilience planning, cooperation mechanisms, and national implementation examples.
- These discussions revealed common obstacles, such as siloed thinking, limited stakeholder involvement, and lack of institutionalized training.
- Several participants contributed existing good practices already tested at national level.

7. Lessons Learned from Previous Incidents

- Experiences from past disruption events were shared to highlight lessons learned.
- Discussions emphasized the need to build on actual incidents to guide future policy and readiness exercises.
- Participants agreed on the value of incident analysis and sharing as essential for collective learning.

8. Building a Community of Practice

- A key takeaway was the importance of developing a trusted network of resilience practitioners across Europe.
- This working group is intended to extend beyond a single workshop, supporting ongoing interaction and support.
- ENDURANCE is seen as the starting point of a long-term cooperation effort across EU regions and actors.

9. Technical and technology related implications for providing resilience

- CE Risk and Resilience standardization process!
- Enhance the CE Risk and Resilience process with cross sector and cross regions assessment mechanism.
- Digitalization\Automation of Risk and Resilience processes. Integration of cutting-edge technologies.
- Continuous and dynamic training and awareness mechanism for CI operators tailored on level of responsibility.

- Enhancement of Cyber-security solutions once with integration of new sensors and solution within the CI environment (IT/OT segmentation). Ensuring the positive impact when integrating new sensors or AI/ML technologies are integrated.
- Integration of a **centralized communication hub** to enhance the communication between cyber agencies, critical operators and authorities.

10. Recommendations for Future Action

- Suggestions included the creation of resilience toolkits, cross-border response protocols, and role-based response training.
- There were calls for a shared resilience maturity model that Member States and sectors could use to benchmark their progress.
- A recommendation was made to organize joint simulation exercises, especially involving operators of essential services.

11. Next Steps and Continuity of Engagement

- The working group will continue through follow-up workshops and thematic sessions.
- Outputs from this session will be compiled and analyzed to inform policy recommendations at the EU level.
- Participants were encouraged to stay involved and contribute actively to upcoming activities, as the project progresses toward concrete outcomes.

Important Reflections from the participants of the EU WS

- “We must not only transpose directives but transform them into effective national practices.”
- “Cross-border resilience depends on cross-border understanding.”
- “Workshops like this help us move from theory to action.”
- “Learning from each other is the most efficient resilience strategy.”
- “There is no resilience without cooperation.”

Action Points & Recommendations

- Support the alignment of national legislation with EU-level resilience directives (NIS2, CER, etc.)
- Create a pan-European repository of lessons learned and good practices.
- Develop sector-specific implementation guides and maturity models.
- Continue roundtable discussions and thematic working sessions throughout the project lifecycle.
- Strengthen permanent communication channels across resilience stakeholders.
- Organize follow-up simulation and training events to test proposed strategies.

5 Conclusion

Deliverable D1.1. provide a detailed collection of analyses and information gathered through different channels. The concept of resilience, structured around the components of **Resistance**, **Robustness**, **Recoverability**, and **Adaptability**, offers a solid foundation for improving the continuity, preparedness, and adaptability of critical infrastructure (CI) and essential service providers (ESP). However, turning this concept into operational capability requires evidence-based inputs, stakeholder engagement, and coordinated action.

Important implications reflect through:

(1) **Insights from National and EU Workshops**: The local (WL1) and European (WE1) workshops provided vital insight into real-world operational challenges, sector-specific vulnerabilities, and national-level differences in policy maturity. These dialogues enabled the direct integration of stakeholder experiences into strategic and operational planning. Such engagement ensures that resilience strategies are not only theoretically sound but also context-sensitive and practically grounded.

(2) **Legal and Regulatory Alignment**: A detailed analysis of existing national and EU-level legislation highlights both gaps and strengths in current frameworks for critical infrastructure protection. The workshops allowed for a comparative discussion of the implementation of the CER Directive, NIS2, and sectoral laws, uncovering ambiguities and inconsistencies that could hinder cross-border cooperation and uniform resilience-building.

(3) **Leveraging Results from Previous EU Projects**: Projects such as ATLANTIS, SUNRISE, PRECINCT, and others have generated rich datasets, tested methodologies, and validated resilience approaches. Incorporating these findings avoids duplication, builds on validated tools, and helps ensure alignment with existing EU-wide innovation efforts. Their results serve as a strategic knowledge base for ENDURANCE and similar initiatives.

(4) **Prepared Use Cases as Testing Grounds**: The development of concrete use cases, based on stakeholder input and real-sector engagement, represents a cornerstone for operationalizing resilience. These scenarios simulate cascading effects, hybrid threats, and digital-physical disruptions, making them ideal testing environments for resilience tools, training, and policy evaluation. They provide a controlled but realistic setting to validate future resilience measures and foster multi-stakeholder collaboration.

(5) **Strategic and Sustainable Impact**: The combination of technical analysis, policy review, stakeholder participation, and practical application provides a comprehensive model for resilience development. It ensures that future systems and strategies are not only compliant and robust, but also adaptive to change, co-developed with users, and capable of responding to increasingly complex threat landscapes.

Resilience in the context of critical infrastructure and cyber systems refers to the ability to withstand, respond to, and recover from adverse events—be they natural disasters, cyberattacks, technical failures, or other disruptions. The concept of resilience can be broken down into four fundamental and

interrelated components: **Resistance**, **Robustness**, **Recoverability**, and **Adaptability**. Each plays a distinct role in ensuring the continuity and security of essential systems and services.

Resistance refers to the ability of a system or entity to withstand disruptive events without significant degradation in performance. It is focused on preventing the occurrence or impact of incidents through proactive measures such as:

- Strong physical and cyber security measures
- Redundancy in system architecture
- Threat detection and prevention mechanisms
- Effective access control and authentication systems

This component is largely preventive and defensive, aimed at minimizing the likelihood that a disruption will penetrate the system.

Robustness is the capacity of a system to continue functioning under a wide range of conditions and stressors. While resistance prevents disruptions, robustness ensures that even when disruptions occur, the system maintains its essential functions. Key characteristics include:

- Fault tolerance and load balancing
- Decentralized and distributed system architectures
- Modular system design that localizes the impact of failures
- Well-documented operational procedures

Robust systems may not avoid disruptions entirely but can absorb the shock without catastrophic failure.

Recoverability defines the ability of a system to return to normal or near-normal functioning within a reasonable timeframe after an incident. This includes rapid restoration of services, repair of damage, and continuity of operations. Critical elements of recoverability include:

- Business continuity plans (BCP)
- Disaster recovery strategies and backups
- Crisis communication procedures
- Post-incident analysis and learning

A strong focus on recoverability minimizes downtime and helps maintain public trust and service reliability during and after disruptions.

Adaptability is the long-term component of resilience. It refers to the system's ability to evolve and improve over time in response to changing conditions, emerging threats, and lessons learned from past incidents. Adaptive systems are dynamic, incorporating:

- Continuous monitoring and feedback loops

- Regular updating of risk assessments and mitigation plans
- Policy and procedural flexibility
- Investment in training and skill development

Adaptability is essential in today's rapidly evolving risk environment and is a core pillar for sustainable resilience.

The concept of resilience, when broken down into its core components Resistance, Robustness, Recoverability, and Adaptability provides a structured and actionable framework for strengthening the stability and continuity of critical infrastructure systems. Understanding and applying these components holistically enables organizations, governments, and service providers to build infrastructures that are not only secure against disruptions but also agile in responding to emerging risks.

Main Implications:

1. Policy Integration:
   National and sectoral resilience strategies must integrate all four components into risk management policies, ensuring that preventive and reactive capacities are equally prioritized.

2. Operational Preparedness:
   Institutions must move beyond technical hardening and incorporate robust operational plans, rapid recovery protocols, and adaptive learning mechanisms into their daily operations.

3. Investment in Capacity Building:
   Sustained investment is needed in workforce training, system upgrades, and research to support dynamic resilience-building efforts over time.

4. Cross-Sector and Cross-Border Cooperation**:**
   Resilience can only be effective when implemented across systems that are interdependent. Stronger collaboration and harmonization among sectors and EU member states are essential.

5. Strategic Foresight and Adaptation:
   With the evolving nature of threats—such as cyber-physical attacks, hybrid threats, and climate-induced events—resilience must be seen not as a static goal but as a continuous strategic function requiring foresight and flexibility.

Building resilience is not solely about recovery; it is about anticipation, resistance, survival, and transformation. Emphasizing all four components enables societies to safeguard essential services, protect populations, and preserve trust in critical systems during times of disruption.

References

1. Brezar, Aleksandar (28 April 2025). "Breaking news. Spain, Portugal and southern France hit by massive power outage". *Euronews*. Archived from the original on 28 April 2025 (https://web.archive.org/web/20250428112520/https:/www.euronews.com/my-europe/2025/04/28/spain-portugal-and-parts-of-france-hit-by-massive-power-outage). Retrieved 28 April 2025.

2. Commission, E. (2024, November). *THE USE OF THE EU EMBLEM IN THE CONTEXT OF EU PROGRAMMES 2021-2027*. Retrieved from https://commission.europa.eu/system/files/2021-05/eu-emblem-rules_en.pdf.

3. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

4. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L333/164 (CER Directive)

5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L333/80.

6. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

7. ENISA. (2024, November). *NIS Directive 2*. Retrieved from European Union Agency for Cybersecurity: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

8. EU HORIZON project SUNRISE, https://www.atlantis-horizon.eu/

9. EU HORIZON project SUNRISE, https://sunrise-europe.eu/

10. EU HORIZON project PRECINCT, https://www.precinct.info/en/

11. EU HORIZON project CORDIS, https://cordis.europa.eu/project/id/833088

12. EU HORIZON project Cyber SEAS, https://cyberseas.eu/

13. EU HORIZON project APPRAISE, https://www.appraise-h2020.eu/

14. Final report on the power system separation of Iberia from Continental Europe on 24 July 2021, https://www.entsoe.eu/news/2022/03/28/final-report-on-the-power-system-separation-of-iberia-from-continental-europe-on-24-july-2021/?utm_source=chatgpt.com.

15. Ferris, Nick (30 April 2025). "Did Spain's push for renewable energy have any impact on its mass power blackout?". *The Independent*. Retrieved 3 May 2025 (https://www.independent.co.uk/climate-change/news/spain-blackout-renewable-energy-solar-wind-b2742000.html).
16. Interconnector Failure in France Causes Outages Across Iberian Peninsula (2021). https://www.theblackoutreport.co.uk/2021/07/26/interconnector-failure-iberian-peninsular-blackout/?utm_source=chatgpt.com.
17. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.
18. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L2847/1.
19. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689.
20. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 [2022] OJ L333/1.
21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
22. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L295/39.
23. Strategic Foresight Report 2020, https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en.

Annex 1: Risk Scenario Requirements Collection

Item	Further description of item	Answer
1 General info		
Use case	What is the risk scenario of your use case?	
Organization	Name of the organization who fill this questionnaire	
Date	Date this questionnaire filled	
Contact method	In case we have some additional questions, in what way can we contact you	
Sector		
Question		**Answer**
Domain	Shortly describe what is the sector in which the organization operate.	
Core Business	What is your core business? On which sector your business mostly rely?	
Employees	How many people works in your organization?	
Customer Base	How many people are included in the customer base of the services offered by your organization?	
Supply Chain	What are the sectors upon which your organization depends? (energy, transportation, etc.)	
Interoperability	What are the sectors with which your organization cooperate?	
Cross Sector Influence	Are there specifics area in the organization that depend on other sectors? What are these sectors?	
Policy framework	Are there specific policies for business continuity in your domain? Are there some policies that differ from the current legislation as NIS2 or DORA?	
Context		
Question		**Answer**

Work methodology	What is the work methodology that is adopted by the organization for its employees (smart working, in-office, hybrid, etc.)?	
Geographical distribution	In how many countries do you have offices? And which is the countries where you have offices?	
Geographical coverage	How many countries do your services serve? And which is the countries that you serve? How many and which nations are in your customer base?	
Threat source	What is the source of your risk scenario? Anthropic, artificial, or natural?	
Threat source	What is the source kind of risk that can cause you more harm in the risk scenario that you have chosen (cyberattack, flooding, internal threat, espionage, etc.)?	
Threat exposure	How many subsystems are involved in the organization's operations? Which subsystems are most critical and vulnerable based in your risk scenario?	
Impact		
Question		**Answer**
Threat propagation	How many Businesses Unit will be compromised by the risk scenario that you've chosen?	
Threat propagation	What is the sector, stakeholder and consumer that will be most impacted by the risk scenario that you've chosen?	
Cross Sector Impact	Is the risk scenario that you've chosen characterized by a cascading effect and could it involve other sectors? What are these sectors?	
Threat and Risk management	Are there some methodologies and strategies adopted by the organization to manage the risk use case scenario that you've chosen?	

Threat and Risk Management	Is there any Business Continuity plan that is involved in the crisis management during the risk scenario that you've chosen? Is there also any Incident response plan?	
Damage level	In case of risk containment and management strategies and methodologies failure are there some disaster recovery plan?	
Time and resilience	How long your services can't be available after the risk scenario that you've chosen impacted the organization, in order to deliver services to the customer in acceptable manner?	
Threat Impact	What is the extent of the damage in the use case scenario that you've chosen? Are involved only operational damages to the equipment or are also involved harm to the people?	
Threat Impact	What is the subsystem that would be more damaged in the risk scenario that you've chosen?	
Probability		
Question		**Answer**
Risk Assessment	Is risk assessment carried out on a regular basis?	
Risk Assessment	Are there some specific business unit and subsystem that are tested more frequently?	
Incident History	Have there been any accidents in the past that fall within the chosen risk scenario?	
Incident History	Are there methodologies and techniques to implement the lesson learned once the accident occurs?	
Awareness and Training	Are there any training programs for the employees related to the risk scenario that you've chosen?	

Threat Probability	What is the probability that the risk scenario chosen impact your organization?	

Annex 2: Questionary for ENDURANCE local workshops

Discussion Panel 1

The insights from the CI stakeholders - resilience in specific sectors of CI (existing policies, strategies, standards, SOP, best practices and business continuity plans defined and/or adopted by the CI authorities and operators)

Resilience concept

Defining resilience:

- How would you define the concept of resilience in the context of your organization or sector?

_____

_____

_____

- What does resilience mean for you in terms of critical infrastructure operations?

_____

_____

_____

Operator/Authority sector

- please indicate the sector in which you act and briefly describe the main activities of your organization related to critical infrastructure resilience.

_____

_____

_____

- What are the potential risks or consequences if the principle of resilience is not applied correctly in your organization or sector?

_____

_____

_____

Resilience area:

- cyber, physical, human -please prioritize the type of risks for your resilience and, where applicable, highlight interconnections between these risk areas in your sector.

_____

_____

_____

Legal framework

Indicate the main policies/directive (local, national, international) that regulate your organization's activities related to resilience.

_____

_____

_____

- Specify those strictly related to the sector in which your organizations belong to:

_____

_____

_____

- What are the reference authorities for your organization regarding resilience (Local or National level)? And how to you communicate with the Authority? Is there a standardized procedure for coordination?

_____

_____

_____

Standard and SOP (Standard Operating Procedure)

- Which are the standards for you organization? Which are mandatory? Which are optional but in use in your organization? (ISO 27001 or other)

_____

_____

_____

- Do you conduct internal and/or external audits related to compliance with these standards or directives? How often are these audits carried out, and what are the key findings?

_____

_____

_____

- Do you have any written and formally approved guidelines or procedures that supplement these standards?

_____

_____

_____

Modus operandi

How is resilience integrated into your sector's strategic or operational planning?

- ☐ Through regular risk assessments and mitigation strategies.
- ☐ By ignoring potential risks and focusing solely on current operations.
- ☐ By outsourcing all resilience planning to external consultants.
- ☐ Other….

Do you have internal policies to implement new directives and regulations on resilience?

- ☐ Yes, we have comprehensive internal policies.
- ☐ No, we do not have any internal policies.
- ☐ We rely on external guidelines without internal policies.

Are the procedures documented and approved? Are there specialized departments or dedicated teams responsible for resilience efforts?

- ☐ Yes, procedures are documented and approved, with dedicated teams in place.
- ☐ No, procedures are not documented or approved, and there are no dedicated teams.
- ☐ Procedures are documented but not approved, and there are no dedicated teams.

How do you ensure proper dissemination and understanding of these policies within your organization?

- ☐ Through regular training sessions and internal communications.
- ☐ By not disseminating the policies at all.

Do you have a methodology to assess the implementation of new policies and directives (National or European)?

- ☐ Yes, we have a robust assessment methodology.

- ☐ No, we do not assess the implementation of new policies.
- ☐ We assess implementation only when issues arise.

What best practices in resilience has your organization adopted?

- ☐ Planning and preparation
- ☐ Collaboration with external stakeholders
- ☐ Regular plan updates
- ☐ Adoption of practices from other sectors or regions
- ☐ Other

How do you test and evaluate the effectiveness of your business continuity plans?

- ☐ Simulations and drills
- ☐ Internal and external audits
- ☐ Employee feedback
- ☐ Collaboration with external experts

What challenges does your organization face in relation to new EU directives, such as NIS2 and CER?

- ☐ Regulatory compliance
- ☐ Limited resources
- ☐ Need for additional support
- ☐ Integration with existing systems

Discussion panel 2

Suggestion for definition and concretization the most representatives use cases connected with providing resilience of CI

Threats evaluation:

1. Please evaluate according to your experience and sector related specifics which threats are the most influenced for providing resilience of your Critical infrastructure? (evaluate each threat with Likert scale 1-lowest influence – 10 - strongest influence

Technical related accidents	1	2	3	4	5	6	7	8	9	10
Natural related threats (floods, wildfires, drought, strong winds)	1	2	3	4	5	6	7	8	9	10
Cyber threats	1	2	3	4	5	6	7	8	9	10
Physical threats (all physical man-made threats)	1	2	3	4	5	6	7	8	9	10
Human related threats	1	2	3	4	5	6	7	8	9	10
Geo-political threats (crisis situations with armed conflicts in the surrounding area	1	2	3	4	5	6	7	8	9	10
Supply chain disruptions	1	2	3	4	5	6	7	8	9	10

2. Have you experienced a risk in the last two years following the COVID-19 period that had a very strong impact on ensuring the resilience of your organization?

If you answered YES, please state what these threats were:

_____

_____

_____

3. If you had the opportunity to design a scenario for a national crisis response exercise to ensure adequate business continuity and resilience in your sector, which risk would be central to your scenario?

Name the two most exposed:

_____

_____

_____

4. Do you think that you can ensure the resilience of your sector through activities and resources within your Critical Infrastructure sector?

☐ YES

☐ No

☐ Partly

5. In your opinion, who should be even more involved in the preparation of test scenarios that would ensure an increase in the resilience of the operation of critical infrastructure and, consequently, the wider social community? (Rate on a scale of 1-10 (1- not at all-10 very important)

Telecommunications sector (operators)	1	2	3	4	5	6	7	8	9	10
Electric power sector	1	2	3	4	5	6	7	8	9	10
First responders (firemen, first aid, police)	1	2	3	4	5	6	7	8	9	10
Health sector	1	2	3	4	5	6	7	8	9	10
Civil protection	1	2	3	4	5	6	7	8	9	10
Other energy sectors (gas, oil)	1	2	3	4	5	6	7	8	9	10
Transport sector (road, railway, maritime)	1	2	3	4	5	6	7	8	9	10
Food sector	1	2	3	4	5	6	7	8	9	10
Drinking water supply sector	1	2	3	4	5	6	7	8	9	10
Financial sector	1	2	3	4	5	6	7	8	9	10
Public administration	1	2	3	4	5	6	7	8	9	10
Other (add)	1	2	3	4	5	6	7	8	9	10

Discussion panel 3

Technology related expectations with influence to stronger resilience of CI

Current tools and their Impact:

- Which existing technology tools in your operational environment do you believe most effectively contribute to risk assessment and resilience of your CI? e.g.: Network monitoring tools, incident response systems, predictive analytics, etc.

_____

_____

_____

Assessment of technology performance:

- On a scale from 1 to 10, how would you rate the efficiency of current technology in supporting the resilience of your CI?

Efficiency of current technology in supporting the resilience of your CI	1	2	3	4	5	6	7	8	9	10

Please explain your rating:

_____

_____

_____

Future technological needs:

- What specific types of technology advancements do you anticipate will be most crucial for enhancing the resilience of CI in the next 3-6 years? *e.g.: AI-driven analytics, enhanced cybersecurity protocols, advanced automation tools, etc.*

_____

_____

_____

- For what critical information useful in the context of the project do you foresee restrictions to share outside your internal environment?

_____

_____

Identification of gaps:

- What major gaps or shortcomings do you currently see in the technology ecosystem and internal processes that impact the resilience of CI? (Open discussion to capture diverse insights.)

_____

_____

_____

User experience and expectations:

- What is your experience in multi-sector and multi-national initiatives? Please give some examples.

_____

_____

_____

- What would be the major obstacles you would foresee in implementing new technologies and processes?

_____

_____

_____

- What features or improvements would you like to see in future technological tools to better support CI resilience? e.g., better integration, user-friendly interfaces, real-time updates and warnings, federated ecosystems, pre-defined procedures/handbooks.

_____

_____

_____

Annex 3: Report and conclusion from EU Cross-Border Collaboration Workshop

Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe

Report and conclusions from EU Cross-border collaboration Workshop

Date: Tuesday March 18th, 2025 (Online)

Time: 9am - 1pm (CET)

Date: 15.04.2025

Status: Final

Content

List of changes

Table 1: List of changes

Version nr.	Date	Change	Author
0.1	29.03.2025	Initial draft	Liana Predut, Adelin Homoraceanu, Aljosa Kandzic, Denis Caleta, Gabriele Giunta, Emilia Gugliandolo, Hans Graux, Amélie Cathier, Emmanouil Mavrogiorgis, Gilda De Marco,
0.2	02.04.2025	Final draft for review	Denis Caleta, Aljosa Kandzic
1.0	04.04.2025	Final version	Denis Caleta, Aljosa Kandzic
1.1	15.04.2025	Final version with participants overview	Denis Caleta, Aljosa Kandzic

Contributors

Table 2: Contributors

Role	Contributor Name	Entity Short Name
Contributor	Liana Predut	EVIDEN RO
Contributor	Adelin Homoraceanu	EVIDEN RO
Contributor	Gabriele Giunta	ENG
Contributor	Emilia Gugliandolo	ENG
Contributor	Emmanouil Mavrogiorgis	SYN
Contributor	Hans Graux, Amélie Cathier	TIMLEX
Contributor	Amélie Cathier	CARCOM
Contributor	Gilda De Marco	INS
Contributor	Aljosa Kandzic	ICS
Contributor	Denis Caleta	ICS

References

Acronyms

Table 3: Acronyms

Acronym	Description
CI	Critical Infrastructure
EU	European Union
CISOs	Chief Information Security Officers
HR	Human Resources
AI	Artificial Intelligence
ML	Machine Learning
DT	Digital Twin

Terms and Abbreviations

Table 4: Terms and Abbreviations

Term/Abbreviation	Description
N/A	N/A

1 Introduction

The ENDURANCE project partners are delighted to announce the organization of the 1st European workshop focusing on Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe.

Cross-sectorial and cross-border collaboration among critical infrastructure operators across Europe is important for providing an adequate level of resilience and business continuity. By aligning with key EU directives (CER directive, NIS-2 directive, DORA…), member states can effectively enhance resilience across the entire European society, which is a primary objective of these regulations.

Understanding the impact of resilience among critical entities extends beyond national borders. Therefore, it is essential to comprehend the roles, processes, and experiences involved through the lens of cross-border cooperation among critical infrastructure providers. This EU level workshop will facilitate discussions aimed at supporting cooperation on a cross-border level to exchange best practices, discuss common issues, and find means for critical infrastructure operators to better support each other in crises.

The outcomes of the discussions will help understand the current operational environment at the cross [1]-border cooperation level, aiming to improve the resilience of critical infrastructure sectors. This analysis will also identify existing gaps and help outline strategies to address them effectively.

The workshop also served as an exceptional opportunity for ENDURANCE project partners to engage with the broader expert community. It provided a platform to communicate the planned steps and identify areas where direct contributions can enhance the project's efforts in conducting a realistic evaluation of the current resilience levels across various EU target environments.

As a natural progression from the local and national workshops conducted by the Greek, Romanian, and Slovenian partners in Novembre and December, we provided this EU workshop as logical additional discussion step.

EU Workshop successfully brought together over 100 Security experts in all security domains, Stakeholders and operators form other Critical Infrastructure organizations, Members of associated Critical Infrastructure projects and other security-related projects and networks, Members of national and international Law enforcement and security agencies and Members of National and international standardization organizations.

The workshop featured five round tables, each focusing on a range of topics relevant to both consortium members and external participants.

Agenda

09.00-09.10: Online WS Welcome opening and Agenda introduction - Dr. Denis Caleta (ICS)

09.10-09.30: ENDURANCE Project introduction – Mrs. Liana-Miruna Predut (EVIDEN) (ENDURANCE Project coordinator)

09.30-09.50: EU-CIP initiative best practices – Mrs. Emilia Gugliandolo (ENG) (EU-CIP Project coordinator)

09.50-10.05: Introduction of Main Conclusions from Local Workshops – Dr. Denis Caleta (WP 1 leader)

10.05-10.15: Coffee/Technical break – Plenary session is divided into virtual tables/sessions

10.15-11.45: Virtual tables/sessions discussions moderated by Cluster Leads ICS, INS, EVIDEN RO & SYN:

ROUND TABLE 1 – Current legal and policy framework - sufficient base for providing resilience of CI – Hans Graux (TIMELEX) with support of Amélie Cathier (CARCOMMUNICATION)

ROUND TABLE 2 – Resilience of the CI from the perspective of strategies and cross cutting interdependences - Gabriele Giunta (ENG) – with support of Emilia Gugliandolo (ENG)

ROUND TABLE 3 – Resilience of the CI from the technical and technology perspective – expectations and integration challenges – Addelin Homoraceanu (EVIDEN) and Emmanouil Mavrogiorgis SYN with support of Liana-Miruna Predut (EVIDEN)

ROUND TABLE 4 – Resilience of CI from perspective of the influence complex threat environment - Gilda De Marco and Paolo Perucci with support of Martina Steffinlongo.
ROUND TABLE 5 – Resilience of CI from the organizational, processual and business continuity plans – Denis Caleta (ICS) with support of Aljosa Kandzic (ICS)

11.45-12.00: Coffee/Technical break – Plenary session is resumed

12.00-12.30: Virtual joint session/sessions discussions reports/key takeaways presented by moderators

12.30-13.00: Reflection and conclusion

Attendees' category:

Registered for the workshop:**165** persons

Visited the workshop: **111** persons

CI & Essential service providers • Electricity • Telecommunication • Port • water • Health	**21** 7 8 2 4 5
IT & Digital	**29**
Government & National Authorities & Regulators & Public Authorities & Local Authorities	**25**
R&D&I	**23**
Policy managers & Lawyers	**4**
Other	**9**

2 Summary of main discussion points and conclusions form round table discussions

2.1 ROUND TABLE 1 – Current legal and policy framework - sufficient base for providing resilience of CI

Five specific topics and questions were prepared and presented for discussion:

1. Scope and Definition of Critical Entities

- **Challenge**: One of the first and most significant issues is determining what constitutes a "critical entity." The CER Directive lays out broad categories such as energy, transport, water, health, and digital infrastructure. However, the definition can be ambiguous in practice, especially for entities that might not fall directly into these categories but still play a vital role in societal functions. Defining what qualifies as critical, especially in sectors with emerging technologies or new services, is complex.

  It was discussed that the CER Directive and NIS 2 Directive aim to strengthen the resilience of critical entities and infrastructures in response to increasing cybersecurity threats, pandemics, and climate change. These directives ensure broader coverage of essential services across Europe.

  A critical entity is any public or private entity designated by a Member State under the directives.

  The designation process is the responsibility of each Member State, which must integrate the directives into their national legislation and appoint critical entities by 18 October 2024, with full implementation required by 17 July 2026.

  Essential service refers to services crucial for maintaining societal functions, economic activities, public health, safety, or environmental stability.

The CER Directive identifies 11 key sectors, as outlined in Commission Delegated Regulation (EU) 2023/2450.

The 11 sectors of the CER Directive can be shown as follows (©Deloitte):

- **Question**: is the scoping sufficiently clear to you? Are you aware of (the need for) broader scoping under national law?

The participants responded that the scoping is clear to them, as experts working in related fields, such as the SUNRISE project. But a significant gap sometimes exists between policymakers and CI operators, who may not fully understand their obligations. This is especially the case in smaller countries with less resources and/or a less strongly developed security culture. Inversely, when there is a strong security culture, implementation is a lot easier, even in small countries (i.e. the key decider is prior culture and experience, rather than size and resources). Projects like ENDURANCE can help practitioners grasp legislation better.

Each Member State must implement and clarify obligations at the national level.

- Member States should define resilience priorities, considering:
    - Cross-border and cross-sector dependencies
    - National vulnerabilities (e.g., climate risks, cybersecurity, energy security)
    - Supervisory bodies & regulators for oversight
    - Natural and human-made risks affecting essential services
    - Geopolitical, technological, and economic threats
    - Risk assessment justification based on national profiles
- Member States must inform critical entities about risks and provide guidance, templates, best practices, and training.

2. Harmonization of Resilience Requirements Across Member States

- **Challenge**: While the CER Directive sets broad guidelines, each EU Member State is tasked with implementing it within their national legal frameworks. There may be differences in how resilience requirements are interpreted and enforced across countries, leading to inconsistencies in how critical entities are regulated within the EU.

  Organizations often fall under multiple legal frameworks, requiring compliance with overlapping but distinct obligations.

  Each regulation has a different focus (e.g., cybersecurity, product security, data protection, financial resilience).

- **Question**: what do you see as the best mechanisms for aligning the interpretation of resilience requirements? Are the mechanisms foreseen by the Directive strong enough?

  It was discussed that more time would be needed to gain experience on these topics, since wide area of different challenges.

3. Coherence – Cybersecurity and Data Protection

- **Challenge**: The CER Directive places significant emphasis on enhancing cybersecurity resilience for critical entities. However, there is a challenge in aligning the directive's provisions with other EU cybersecurity and data protection laws, such as the **General Data Protection Regulation (GDPR)**, the **NIS2 Directive,** the **AI Act,** and the **CRA**. Ensuring that cybersecurity measures are sufficient while respecting privacy rights and data protection laws is a key legal issue.
- **Question**: are these instruments sufficiently aligned, in your perspective, and are there measures in your country that facilitate coherent interpretation and application?

It was discussed that some countries have initiated discussions between Data Protection Authorities (DPA) and National Security Coordinators to align cybersecurity and data protection requirements. This seems like a good practice for other Member States to avoid disparities.

Due to low participation and technical issues (participants were unable to use their microphones), the breakout discussion was cut short at this point. Future discussions with larger groups are needed for a more meaningful exchange on alignment challenges.

The following topics were also prepared, but not discussed during the session:

4. Implementation of Operational Resilience Measures – laws and realities

- **Challenge**: The directive requires critical entities to take measures to ensure their operational resilience, including assessing risks, implementing security measures, and having contingency plans in place. However, there is ambiguity about the practicalities of implementing these measures, particularly in terms of balancing the cost of compliance with the level of resilience required.
- **Question**: the CER Directive is a legal instrument, that requires strong operationalization. Typically, legal expertise and operational practice don't often mix well. What best practices do you know of for translating laws into operational reality? Do you expect the CER Directive do be effective on this point?

5. Enforcement and Liability for Non-Compliance

- **Challenge**: A key issue is ensuring that the resilience measures are not just put in place but are actually followed and enforced. The CER Directive calls for Member States to establish competent authorities to monitor compliance and enforce penalties for failure to comply. However, there is ambiguity around the enforcement mechanisms, penalties, and legal liability in the event of a failure in resilience, particularly in cross-border situations.
- **Question**: how could Member States effectively enforce the rules against operators that fail to meet the imposed standards (effective in the sense that they elevate resilience, rather than just punishing noncompliance)?

2.2 ROUND TABLE 2 – Resilience of the CI from the perspective of strategies and cross cutting interdependences

Discussion points and questions:

- Q1.1: How can cross-sector and cross-border collaboration be enhanced in light of the increasing interdependencies of critical infrastructures across multiple domains?
- Q1.2 How can these strategies be adjusted to address emerging threats such as cyber, physical and hybrid threats as well as systemic risks?
- Q2.1: How can public-private partnerships promote investment in resilient infrastructure and innovation?
- Q2.2: How can different stakeholders collaborate better to enhance response and readiness capabilities?
- Q3: How can methods for risk assessment and resilience be improved to provide a more comprehensive understanding of the vulnerabilities and interdependencies present in critical infrastructure networks?
- Q4.1: How might machine learning and artificial intelligence improve threat identification and situational awareness for the protection of critical infrastructure?
- Q4.2: What are the major risks of implementing these technologies in settings mission-critical environments?

ROUND TABLE 2: TAKE AWAYS

- Resilience of Critical Infrastructure (CI)
- Strategies must go beyond policymaking to include technical solutions.
- Cross-sector and cross-border interdependencies are increasing, making resilience more complex.
- Three pillars for enhancing collaboration:
  - Policy and Protocols: Unify protocols to reduce fragmentation.
  - Technologies: Interoperable communication systems and automation of response to attacks.
  - Validation & Lessons Learned: Incorporate best practices, involve operators and authorities more deeply.

Addressing Emerging Threats (Cyber, Physical, Hybrid, Systemic)

- Growing complexity of hybrid threats (e.g., EU-HYBNET project).
- Legislation is a key concern: Many sector-specific regulations exist, but fragmentation remains.
  - Example: CS in the Energy Sector via NIS2.

  - The MELICERT program was launched by the EU in 2024 but lacks coordination with ENISA.

- Risk Management must be dynamic:
  - Continuous review and adaptation of frameworks.
  - Expanding risk assessment beyond traditional threats to include a holistic view.
  - Operators must be actively involved in shaping policies and responses.

Enhancing Public-Private Partnerships (PPP) for Resilience Investment

- PPP is essential for:
  - Risk-sharing and leveraging complementary expertise.
  - Encouraging investment in resilient, future-proof solutions.
- Regulatory compliance & security culture are crucial:
  - Standardization of approaches.
  - Empowering stakeholders to actively engage in resilience efforts.

Improving Stakeholder Collaboration for Readiness and Response

- Better information-sharing mechanisms
- Joint risk assessment methodologies
- Leveraging advanced technologies (AI, predictive analytics) for faster and more effective response
- Secure communication channels for intelligence sharing
- Cultural shift toward proactive security.

AI & Machine Learning for Threat Identification & Situational Awareness

- AI and ML can significantly enhance:
  - Threat detection and situational awareness
  - Physical and cyber security measures
  - Federated Machine Learning (FML) as a solution to reduce bias.
- Challenges & Risks:
  - Regulatory compliance: AI must align with national laws.

- Bias in AI/ML models can lead to wrong predictions.
- Data availability and quality impact effectiveness.
- Keeping human operators in the loop is crucial to mitigate AI errors.

Future Directions & Action Points

- Reduce fragmentation of regulations and foster cross-sector collaboration.
- Enhance AI training transparency and ensure bias mitigation.
- Promote cross-border collaboration through standardized digital systems.
- Encourage proactive resilience measures and automate response mechanisms.

2.3 ROUND TABLE 3 – Resilience of the CI from the technical and technology perspective – expectations and integration challenges

Q1 – Improving CI resilience assessment

- What are the current mechanisms for assessing the resilience of your entity? How can the assessment mechanism be improved to improve cross-sectoral or cross-country resilience assessment (risk assessment tools/automation)?

Backup question:

- What are the essential SW or HW components of your resilience mechanism that support the continuous operation of critical infrastructure during major disruption?

Q2 – Training and Awareness

- What are the key components of an effective training program for critical infrastructure workers, and how can it be adapted to address specific sector needs? -> e.g., VR/AR, serious gaming, critical entity training simulation environment

Backup:

- What integration challenges might arise when implementing advanced training programs for critical infrastructure workers, and how can these challenges be addressed to ensure comprehensive and effective training and awareness?

Q3 - Interdependencies between sectors/cascading effects between sectors/other regions or countries

- What is the current process to assess the interdependencies between other sectors and other regions/countries and any potential impacts of a critical event?
- What challenges does the Modernization of Legacy Infrastructure pose towards its resiliency? What are some methods you use to maintain your levels of resiliency when upgrading & digitizing old non digital infrastructure?

Backup:

- Which are the advanced technologies expected to connect different sectors and geographies, and what challenges might arise from integrating these technologies?

Q4 – Cybersecurity – solutions for resilience improvements.

- What are the current gaps between your internal processes and procedures and the NIS2 directive?
- How does your organization ensure that their critical infrastructure is set up and prepared for emerging threats in the context of IT/OT segmentation?
- Do you use automation to increase the level of your entity's security? Do you believe this is proven to be useful?

Q5 – Mechanisms/solutions for collaboration between Critical infrastructure authorities and operators at local/national/EU level

- What are the key technological components required to establish secure and efficient communication channels between critical infrastructure operators and authorities at local, national, and EU levels? What are the current gaps here between entities?
- Would a mechanism to automatically check the impact assessment of a security incident across the critical infrastructure at the national level be helpful for you?

We will concentrate on round table no. 3, which addresses CI resilience from technical and technological perspectives, focusing on expectations and integration challenges.

The discussions were engaging and interactive, featuring contributions from participants both live and via chat.

After a brief overview of the key entities and sectors encompassed by NIS2, along with its compliance pillars and relevant KPIs for resilience improvement, we delved into the core topics.

Here are the 5 topics constituting round table no 3 of the 1st Endurance EU workshop:

- Topic 1 – Improving CI resilience assessment

- Topic 2 – Training and awareness
- Topic 3 – Interdependencies/cascading effects between sectors/other regions or countries
- Topic 4 – Cybersecurity solutions for resilience improvements
- Topic 5 – Mechanisms/solutions for collaboration between CI authorities and operators at local/national/EU level

Topic 1 – Improving CI resilience assessment

The question raised during this topic discussion: "What are the current mechanisms for assessing the resilience of your entity? How can the assessment mechanism be improved to enhance cross-sectoral or cross-country resilience assessment (risk assessment tools/automation)?"

Current risk assessments are conducted primarily at the sector or even the operator level and it is unclear if there is a resilience process in place at the operator level.

The key challenges identified include:

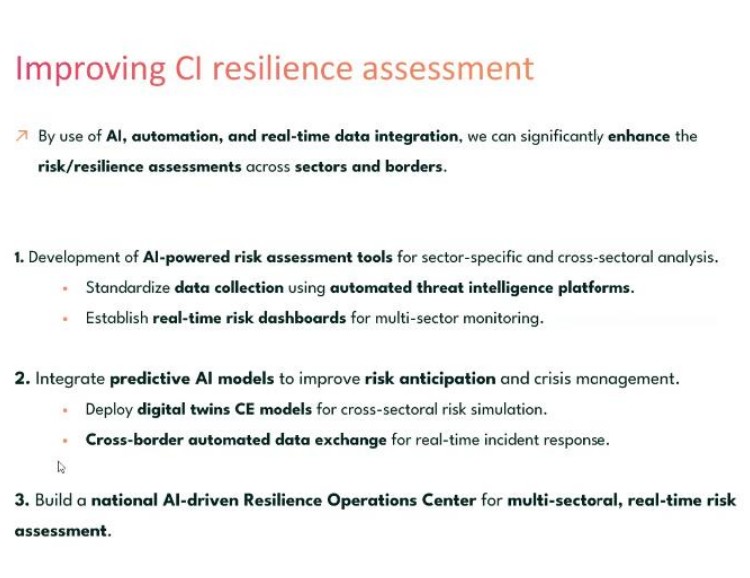
- Lack of a standardized process to assess risk at the sector level and understand the interdependencies between sectors
- Results are not collected in a digital format
- No established risk assessment or resilience framework at the ecosystem level

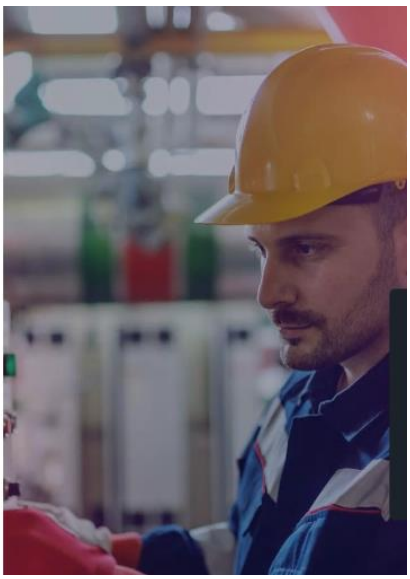
Additional perspectives are collected from SYN, respectively INS representatives stressing out that:

(SYN) resilience assessment by individual entities is different in terms of mechanisms from one entity to the other. Assessment is performed at scale, and it depends on the size of the institution, which is why it is important to implement cross-country and cross-sectoral mechanisms for assessment. **Standardization is key.**

(INS) resilience assessment also depends on the extent of the area of the CI covered (for instance, evaluations are not performed in the same way at municipality level as the geographical level and even the latter is heterogenous). Within the same geographic area, risk assessment mechanisms (tools, methodologies) depend on the concerned sectors – some issues can affect all sectors in a specific area, others not. So, taking into consideration the cascading effects and the consequences of potential issues/incidents is very important when performing assessments.

3 proposals are advanced by the host (EVI-RO) for improving CI resilience assessment:





Additional perspectives related to these first proposals are collected from SYN, INS, respectively ATOS/EVI representatives stressing out that:

(EVI/ATOS) suggests standardization in terms of processes and data collection-related processes since different countries are involved. To mitigate this, a unique data model will be defined at the project level (the aim is to split the model in the Digital Twins models and to assess the interdependencies between sectors.)

Also, modeling with the know-how from operators is very important.

(INS) states that option 2 (predictive AI) would bring the most value when it comes to developing models to assess impact on web platforms.

Also, the digital twin option is reinforced as perfect for mirroring the risk and observing its potential implications. However, it can also be challenging due to flexibility of the CI in different directions and the unpredictable nature of the events that can affect organizations as well as the DT in the integration process. A counter measure to mitigate this challenge would be to address its modelling with a lot of care and equip it with strong updates (contextual input specifically) and dynamicity woven into it.

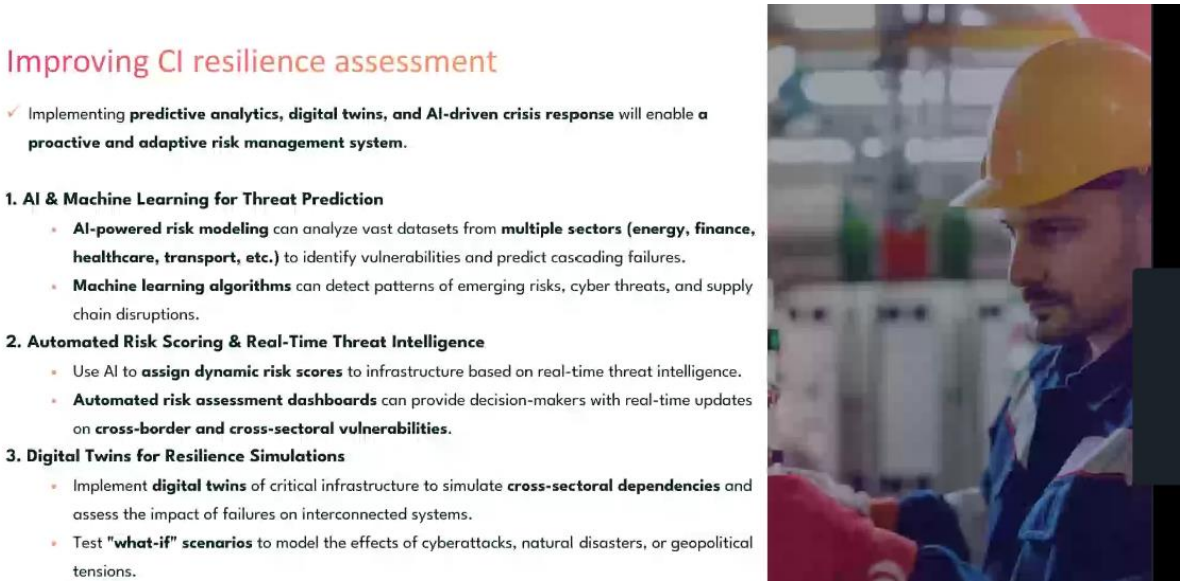
(SYN) states that the addition of digital twins might have negative impact for risk assessment as well as post-incident analysis purposes.

Additional perspectives collected from chat on this topic state that:

(Faculty of security studies University of Belgrade) successful risk assessment involves working closely with Chief Information Security Officers (CISOs), HR teams, and executive leadership to ensure risk intelligence aligns with business priorities and compliance requirements. Risk teams are often required to act on incomplete information during disturbances and crises.

(EYDAP SA) AI combined with ML technologies might help in predictive maintenance and risk anticipation.

A second set consisting of 3 proposals for improving CI resilience assessment is advanced by the host (EVI-RO):



Additional perspectives related to the second set of proposals are collected stress out that:

(INS) option 1 (AI/ML) and 3 (DT) are most important for improving resilience assessments

(SYN) AI must keep humans in the loop on a general note and for final decision making - AI act is very strict

Participants express concerns regarding AI-powered options that have limitations due to their vulnerabilities as well as ML-related threats caused by exploitability. The mitigation measure proposed would be to implement a warning mechanism whenever an AI/ML mechanism is exposed.

Topic 2 – Training and awareness

The question raised during this topic discussion: “What are the key components of an effective training program for critical infrastructure workers? How can we adapt it to address specific sector needs? (e.g.: VR/AR, serious gaming, critical entity training simulation environment)”

In the context of identifying the most valuable training types to complement the awareness process, participants provide the following examples of types of training for employees which were very successful:

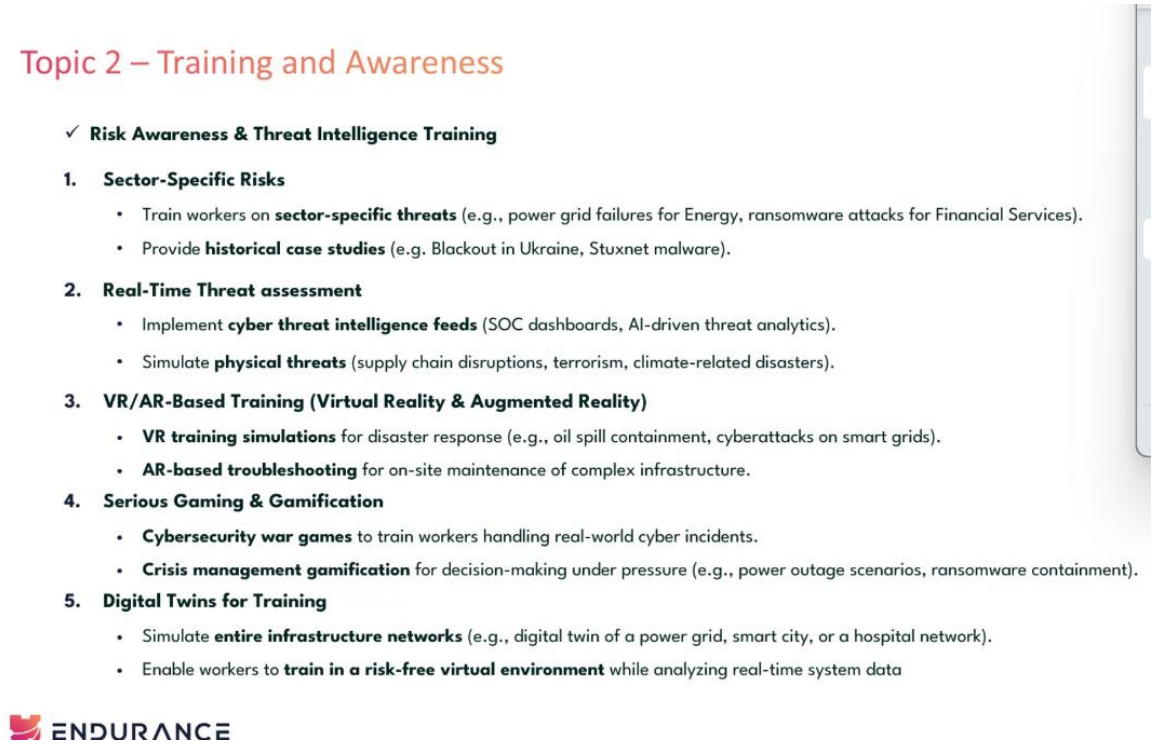
(INS) states that video-training and test quizzes as final assessments (gamification techniques)

Both INS and EVI-RO stress out that cyber training is very important as is raising awareness to prepare for cyber-attacks both for the workers and the top management. However, there must be a differentiation between training and exercise modules conceived for employees and for top level management (high-risk data, protecting core business metrics, sensitive data, etc.)

EVI-RO: phishing tests received on the company email (reported by the security officer)

EVI-DE: simulate the knowledge (gamification technique again) through a DT with all service catalogues integrated into it, plus an assessment scale and real data fed into it, followed by a lot of "what if analysis".

5 proposals are advanced by the host (EVI-RO) for identifying the most valuable training and awareness resource per sector:



(INS) states the 1st (sector-specific risks), 2nd (real-time threat assessment), and 5'th (digital twin for training) options are the most important.

Topic 3 – Interdependencies/cascading effects between sectors/other regions or countries

The questions raised during this topic discussion were:

- "What is the current process to assess the interdependencies between other sectors and other regions/countries and any potential impacts of a critical event?"
- "What challenges does the Modernization of Legacy Infrastructure pose towards its resiliency?"
- "What are some methods you use to maintain your levels of resiliency when upgrading & digitizing old non-digital infrastructure?"

Topic 3 aimed to understand the current process that addresses the interdependencies between sectors (if any) and whether each operator has a good grasp of this information:

(INS) mentions that it is difficult to assess interdependencies between sectors. For them, the perspective is not so much inter-sectorial as they focus more on the vital services, they require to stay

functional (for instance, they cannot provide their services without energy. In turn, this will impact all digital services at the region level as there are no cross-region or cross-sector analysis and prevention mechanisms in place, leading to the snowball effect).

Participants agree that cascading effects are best observed during crisis situations (for instance, the pandemic).

INS also highlights that cooperation mechanisms are missing and need to be cultivated between regions (at the company level between regions), but there is a lot of reluctance. For instance, people working in energy, water, government facilities, etc. tend to NOT come together in requesting a unified platform for resilience with CI data centers operated at pan-European level.

A centralized approach on resilience (and resilience assessment, implicitly) and cooperation is missing – tools, mechanisms, solutions are needed to improve the interdependency analysis between sectors.

(SYN) mentions that there are also risks associated to the digitalization of critical infrastructures (for example, sensors) since this means that entities now get exposed to risks that they did not face before.

Public administration representatives (analyst perspective) state that they introduced a web application (for car systems) that can flag vulnerabilities to better overcome this gap. The assigned workers will need training, and a gap analysis would also be beneficial when moving from an old (analog system) to a digital one.

A final example provided by the same public administration refers to internal phishing simulations to mitigate potential challenges related to the digitalization process (as cybersecurity starts with the people as the biggest threat).

Topic 4 – Cybersecurity solutions for resilience improvements

The questions raised during this topic discussion were:

- "What are the current gaps between your internal processes and procedures and the NIS2 directive?"
- "How does your organization ensure that its critical infrastructure is set up and prepared for emerging threats in the context of IT/OT segmentation?"
- "Do you use automation to increase the security level of your entity? Do you believe this is proven to be useful?"

(INS) When it comes to gaps between the current process and the process recommended by NIS2, they would benefit from increasing the frequency of risk assessments.

Preparedness at organizational level in the context of IT/OT segmentation is another important topic to consider here.

Finally, when referring to specific types of automation that can increase the security level of entities, the Serbian perspective emphasizes the importance of increasing the level ok skills and awareness for people in charge of automation processes. Boasting a balanced level of expertise and skillfulness within the sector and ensuring that people are prepared for emerging threats is essential.

Other types of automation that can help strengthen the security level of entities: incident response mechanisms, automated assessment of any threats to cyberspace, etc.

Topic 5 – Mechanisms/solutions for collaboration between CI authorities and operators at local/national/EU level

The questions raised during this topic discussion were:

- "What are the key technological components required to establish secure and efficient communication channels between critical infrastructure operators and authorities at local, national, and EU levels? What are the current gaps between entities from this perspective?"
- "Would a mechanism to automatically check the impact assessment of a security incident across the critical infrastructure at the national level be helpful for you?"

Such mechanisms are not used today or are missing entirely. Some of the mitigation options proposed by the host include:

- a dedicated CI network to be used for information exchange
- an end-to-end encrypted channel to exchange data
- ZTNA network
- private 5G network
- satellite support
- emergency radio system where possible
- centralization tools necessary to create communication between cyber agencies, critical operators and authorities (**centralized communication hub** and communication mechanisms between critical operators and authorities)

Additional perspectives related to these first proposals are collected from INS, University of Belgrade, Eviden:

For the centralized communication hub, standardization in terms of regulatory framework and more is essential.

A centralized communication hub can be very useful as many analysts could access and maintain a lifeline communication with authorities for sectoral events and continuous information sharing.

(INS) mentions that if something changes in the communication methodology when using the centralized tool, the changes must be reflected at the organization level as well – so new technology, new task, new skill, and continuous syncing between centralized hub and public entities, policy makers, and public CI operators even more then for private companies and CI operators.

Additional contributions were also collected from the round table's chat:

INS also mentions the **integration with other tools**, like Service Now, JIRA, etc. Thus, ideas targeting different integrations gain momentum (for instance, a voice mentioned the implementation of a ticketing platform with risk assessment options to maintain active and collaborative feedback loops).

(EVI-DE) mentions the addition of multilingual support to the platform, particularly in the context of increased immigration in Europe.

Finally, the University of Belgrade stresses out that a differentiation between risk vs crisis communication is paramount and this transition is essential for the establishment of successful collaboration mechanisms across the EU.

Takeaways

- CE Risk and Resilience standardization process!
- Enhance the CE Risk and Resilience process with cross sector and cross regions assessment mechanism.
- Digitalization\Automation of Risk and Resilience processes. Integration of cutting-edge technologies.
- Continuous and dynamic training and awareness mechanism for CI operators tailored on level of responsibility.
- Enhancement of Cyber-security solutions once with integration of new sensors and solution within the CI environment (IT/OT segmentation). Ensuring the positive impact when integrating new sensors or AI/ML technologies are integrated.
- Integration of a **centralized communication hub** to enhance the communication between cyber agencies, critical operators and authorities.

2.4 ROUND TABLE 4 – Resilience of CI from perspective of the influence complex threat environment

Discussion points:

Main environmental threats that could affect the resilience of our critical infrastructures

. Extent of the impact of an extreme environmental event on service delivery (economic/social implications)
. Mitigation strategies to protect critical infrastructures from environmental threats
. Role of public and private sectors in enhancing the resilience of critical infrastructures/investment priorities to increase resilience
. Emerging technologies that can be used to monitor and respond to environmental threats

This round table wasn't provided with additional discussion due to the small number of interested participants. We re-organize activities and will postpone and use this topic for the next European Workshop discussion!!!

2.5 ROUND TABLE 5 – Resilience of CI from the organizational, processual and business continuity plans

Discussion points and questions:

Organizational Resilience:

Q1. How can leadership ensure that resilience becomes a core part of the organization's culture, rather than just a compliance requirement?

Points for discussion:

Leadership Commitment: Leaders must champion resilience as a strategic priority, not just an operational necessity. This means integrating resilience goals into the organization's vision, mission, and performance metrics.

Training and Awareness: Regular training and awareness programs should help employees at all levels understand their role in safeguarding critical infrastructure.

Cross-Departmental Collaboration: Breaking down silos between IT, operations, and management ensures resilience strategies are holistic and practical.

Resilience Champions: Appointing dedicated resilience officers or teams can help sustain focus and momentum.

Incentives and Recognition: Rewarding proactive risk management and innovative resilience ideas encourages employees to prioritize resilience.

Processual Resilience:

Q2. What key performance indicators (KPIs) can be used to measure the effectiveness and adaptability of critical infrastructure processes during disruptions?

Additional points for discussion and reflection of some powerful KPIs:

Mean Time to Recovery (MTTR): How fast can processes recover from disruption?

Process Downtime Percentage: Total downtime compared to standard operational hours.

Incident Detection Time: How long does it take to detect an issue?

Process Redundancy Readiness: The number of critical processes with tested backups.

Supply Chain Stability: The number of backup suppliers/processors available for critical components.

Employee Response Time: How quickly are incident protocols activated by staff?

Business Continuity Planning:

Q3. How frequently should business continuity plans be tested and updated to remain effective against emerging threats, including cyberattacks and physical disruptions?

Additional points for discussion:

Frequency: Best practices suggest running full continuity tests annually, with quarterly tabletop exercises and monthly checks on critical components (e.g., backups, redundant systems).

Triggered Reviews: Any major changes — like infrastructure upgrades, mergers, or new threat landscapes — should immediately trigger a BCP update.

Diverse Scenario Testing: Rotate between natural disasters, cyberattacks, insider threats, and supply chain failures to cover different vulnerabilities.

Third-Party Validation: External audits provide unbiased insights and help spot overlooked weaknesses.

Post-Incident Reviews: Each real-world disruption should lead to immediate adjustments to the BCP.

Interdependency Management:

Q4. How can organizations map and manage interdependencies between different critical infrastructure sectors to prevent cascading failures?

Dependency Mapping: Create a visual map showing all interconnected systems, suppliers, and processes. Identify "single points of failure."

Risk Prioritization: Categorize interdependencies by impact and likelihood of failure.

Redundancy Planning: Build redundancies for essential services and ensure third-party suppliers also have resilience plans in place.

Inter Organizational and Cross-Sector Collaboration: Work with other CI sectors (e.g., energy, telecommunications, transportation) to ensure collective resilience, especially in regional or national infrastructure ecosystems.

Real-Time Monitoring: Use IoT sensors and predictive analytics to monitor interconnected systems and detect anomalies early.

Technology and Automation:

Q5. What role do emerging technologies — such as AI, IoT, and blockchain — play in strengthening the resilience of CI, and what are the potential risks of over-relying on automation?

Benefits:

AI: Enables predictive maintenance, anomaly detection, and rapid threat analysis — reducing downtime and response times.

IoT: Real-time data from smart sensors improves situational awareness and process visibility, allowing for faster decision-making.

Blockchain: Enhances supply chain transparency and data integrity, reducing fraud and ensuring trustworthy data flows during disruptions.

Risks:

Single-Point of Automation Failure: Over-reliance on AI and automation could create new vulnerabilities — if the AI fails or gets hacked, the entire infrastructure could collapse.

Cyberattacks on IoT: IoT devices are often targeted by attackers. Poorly secured devices could serve as an entry point for large-scale breaches.

Blockchain Scalability Issues: While secure, blockchain networks can face performance issues under high loads, potentially slowing down recovery processes.

Human Expertise Dilution: Excessive automation may lead to skill degradation among human operators, leaving organizations vulnerable if systems fail and manual intervention is required.

Discussion Topics and conclusions

1. Resilience as a Strategic Priority

- The main theme revolved around resilience from organizational, procedural, and operational perspectives.
- The importance of aligning business continuity plans with real-world threats such as cyberattacks, pandemics, and natural disasters.
- The need for operational flexibility to ensure organizations can rapidly adapt during crises without compromising core services.
- Organizations are aiming to embed resilience into daily operations, making it an ongoing mindset rather than a checkbox item.
- Denis Čaleta emphasized that resilience should be built across multiple levels—within organizations, nationally, and across the EU—as part of a layered defense strategy.
- The group also touched on supply chain interdependencies and the risk of cascading failures, especially across critical infrastructure that spans national borders.

2. Cybersecurity & Continuity Planning

- Cybersecurity is a fundamental pillar of resilience, especially from a national policy and auditing perspective.
- Cybersecurity should not be an isolated function but integrated into the overall risk and continuity framework.
- There is a need for continuous auditing and updates of security controls and processes as threats evolve.

- Organizations must improve cyber literacy among leadership, as executive awareness often lags behind technical developments.
- Integration of cybersecurity into business continuity and incident response was also debated, with suggestions for simulating cyber scenarios during BCM exercises.
- Panelists shared insights about periodic reviews and real-world testing of business continuity and cybersecurity procedures as required by national policy.

3. Cross-Border Coordination

- Coordinating across national and institutional boundaries during crises remains a challenge.
- Inter-organizational and cross-border collaboration must be pre-planned and rehearsed, not improvised during incidents.
- Difficulties include information-sharing, misaligned national procedures, and unclear decision-making roles when infrastructure or services cross jurisdictions.
- The importance of bilateral frameworks between neighboring infrastructures was discussed, particularly for EU and non-EU collaborations.
- Participants stressed the need for joint preparedness exercises and communication protocols that would function under pressure.

4. Workshop Value & Knowledge Exchange

- The interactive and peer-driven format of the workshop was highly praised.
- Provided a platform for exchanging national practices, methodologies, and challenges.
- Offered fresh ideas about evaluating resilience, including scenario-based testing and lessons learned reviews.
- Encouraged practical collaboration between partners for co-developing response frameworks and shared methodologies.
- Interest was expressed in organizing future collaborative exercises such as tabletop simulations and co-authored guidance documents.

5. Leadership, Governance & Strategic Alignment

- Leadership plays a central role in operationalizing resilience across all organizational layers.
- Resilience must be driven from the top and be part of strategic decision-making.
- Disconnects between strategy and implementation were identified as a frequent challenge.
- Boards and C-level leadership should treat resilience as an ongoing governance responsibility.
- Governance frameworks must ensure accountability for both planning and execution.

6. Testing, Metrics & Continuous Improvement

- Resilience should be evaluated through real-world scenarios and iterative improvements.
- Organizations should track metrics such as downtime, recovery times, and scenario success rates.
- Testing must reflect current threat landscapes and not just historical events.
- Business continuity plans must evolve based on lessons learned from incidents and exercises.
- Avoidance of box-ticking exercises was emphasized; realistic testing brings real resilience.

7. Human Factors, Culture & Internal Awareness

- People are the most critical component of resilience — not just systems or policies.
- Communication failures during crises underscore the need for simple, well-known protocols.
- Resilience culture must be cultivated through active engagement and ongoing awareness.
- Employees at all levels should participate in drills, debriefs, and planning processes.
- Training should go beyond compliance and include gamified or scenario-based approaches.

8. Policy Harmonization & Regulatory Alignment

- Policy discrepancies between countries hinder effective cross-border resilience.
- EU and non-EU harmonization efforts should be prioritized to create inclusive frameworks.
- Participants suggested building modular policy toolkits for varying levels of readiness.
- Policy alignment helps reduce friction and uncertainty during joint responses.
- Projects like this can serve as incubators for developing transnational policy recommendations.

9. Innovation, Emerging Threats & Future Readiness

- Resilience strategies must adapt to new threat vectors, including AI, misinformation, and hybrid attacks.
- Forward-looking planning was encouraged to account for 'black swan' and low-frequency events.
- Innovation should be welcomed — but with an awareness of its impact on resilience.
- Participants discussed tools like predictive modeling and automation for risk management.
- Future resilience planning must remain agile to incorporate emerging technologies and scenarios.

10. Inclusiveness, Participation & Value of Diverse Perspectives

- The session demonstrated how diversity of roles, geographies, and institutions enriches discussions.
- Participants valued the inclusive environment that allowed even those with tech issues to contribute.
- Involving stakeholders from smaller or underrepresented entities adds realism and practical insights.
- Future workshops should continue to prioritize inclusive participation and horizontal learning.
- Inclusiveness ensures resilience frameworks reflect real-world complexity and variation.

Action Points & Recommendations

1. Enhance internal testing of business continuity and cyber resilience plans through realistic and frequent exercises.
2. Leaders must foster a mindset where resilience is seen as a continuous journey — not a one-time project.
3. The goal is to track not just recovery speed but also how adaptive and proactive the processes are.
4. BCPs are living documents they must evolve with emerging risks and operational changes.

5. Resilience is only as strong as the weakest link mapping and safeguarding interdependencies is vital.
6. Balance is key leverage emerging tech for efficiency but keep human oversight and backup mechanisms in place.
7. Develop shared response templates that can be adapted across partner countries and institutions.
8. Incorporate cybersecurity auditing into all levels of resilience planning, from local systems to national infrastructure.
9. Foster collaboration on real-life case studies and organize joint workshops focused on applied learning.
10. Train leadership to understand and promote resilience as a strategic enabler not just a risk mitigation exercise.
11. Create bilateral/multilateral coordination protocols, especially where infrastructure and services cross borders.

3 Conclusions and summary of key insights from EU workshop discussions

The EU workshop enabled a multifaceted approach to presenting the key highlights addressed by the ENDURANCE project. In the first phase, the introductory part of the European workshop provided an appropriate presentation of the project's key steps and objectives. The main highlights from the implementation of national workshops across four countries—Greece, Italy, Romania, and Slovenia—were presented, alongside the establishment of corresponding pilot environments. Additionally, a presentation of the EU-CIP partner project was conducted, showcasing ENDURANCE's significant contribution to the repository of best practice examples in the field of critical infrastructure protection.

Besides introducing the initial steps for further discussion in later roundtable sessions, the first part also served as a fundamental briefing for the members of the Pan-European Working Group on Disruption Resilience.

In the second part of the EU workshop, the focus was entirely on opening a discussion about key aspects of ensuring the resilience of critical infrastructure. An in-depth discussion took place within the framework of four roundtable sessions. However, due to an insufficient number of participants registering for the roundtable dedicated to risk assessment, the organizers decided to postpone this topic and feature it as one of the leading discussions at the next EU workshop.

The previous section of the report provides a detailed overview of the discussion topics, summaries, and recommendations for the next steps related to strengthening critical infrastructure resilience. All inputs gathered will also play a significant role in drafting the European strategy for critical infrastructure resilience.

In the following section, we will outline some of the broadest conclusions from the discussion. All details are available in the recorded discussions from each roundtable session.

1. Purpose and Vision of the ENDURANCE Project

- The project aims to enhance strategic cooperation and create a pan-European platform for resilience coordination.
- Its focus is on exchanging best practices, knowledge, and experiences related to the resilience of critical services.
- One of its primary goals is to support EU Member States in implementing legal frameworks such as the NIS Directive, CER Directive, and others.
- The project includes 12 national workshops and 3 EU-level events, with this being one of the first.

2. Structure of the Workshop

- The session began with three key presentations, followed by a division into five virtual roundtables, each focused on a distinct theme.
- Participants were invited to engage in honest, in-depth discussion on challenges, lessons learned, and practical experiences.
- The roundtables were designed to foster idea generation, identify gaps, and produce actionable insights for resilience-building.

3. Harmonization of Legal and Strategic Frameworks

- A core topic was the need to harmonize national approaches to resilience with existing EU directives.
- Participants discussed the challenges of transposing EU-level documents into national legislation, and how alignment remains uneven.
- The goal is to streamline understanding and implementation across sectors and countries for more effective coordination.

4. Strategic Communication and Coordination

- The session underlined the importance of strategic-level coordination across public and private entities.
- Effective resilience planning was said to rely on continuous, structured communication, not only during crises.
- Roundtable discussions emphasized the value of mutual support and information-sharing before, during, and after disruptive events.

5. Sectoral Implementation Challenges

- Participants shared challenges in adapting resilience frameworks to different sectors (e.g. energy, water, transport, digital).
- The group acknowledged that sector-specific needs must be balanced with unified EU guidance.
- Discussions covered gaps in technical resources, knowledge, and the operationalization of policy into practice.

6. Roundtable-Based Knowledge Exchange

- Each breakout session produced practical input on key topics such as resilience planning, cooperation mechanisms, and national implementation examples.
- These discussions revealed common obstacles, such as siloed thinking, limited stakeholder involvement, and lack of institutionalized training.
- Several participants contributed existing good practices already tested at national level.

7. Lessons Learned from Previous Incidents

- Experiences from past disruption events were shared to highlight lessons learned.
- Discussions emphasized the need to build on actual incidents to guide future policy and readiness exercises.
- Participants agreed on the value of incident analysis and sharing as essential for collective learning.

8. Building a Community of Practice

- A key takeaway was the importance of developing a trusted network of resilience practitioners across Europe.
- This working group is intended to extend beyond a single workshop, supporting ongoing interaction and support.
- ENDURANCE is seen as the starting point of a long-term cooperation effort across EU regions and actors.

9. Technical and technology related implications for providing resilience

- CE Risk and Resilience standardization process!
- Enhance the CE Risk and Resilience process with cross sector and cross regions assessment mechanism.
- Digitalization\Automation of Risk and Resilience processes. Integration of cutting-edge technologies.
- Continuous and dynamic training and awareness mechanism for CI operators tailored on level of responsibility.
- Enhancement of Cyber-security solutions once with integration of new sensors and solution within the CI environment (IT/OT segmentation). Ensuring the positive impact when integrating new sensors or AI/ML technologies are integrated.
- Integration of a **centralized communication hub** to enhance the communication between cyber agencies, critical operators and authorities.

10. Recommendations for Future Action

- Suggestions included the creation of resilience toolkits, cross-border response protocols, and role-based response training.
- There were calls for a shared resilience maturity model that Member States and sectors could use to benchmark their progress.
- A recommendation was made to organize joint simulation exercises, especially involving operators of essential services.

11. Next Steps and Continuity of Engagement

- The working group will continue through follow-up workshops and thematic sessions.

- Outputs from this session will be compiled and analyzed to inform policy recommendations at the EU level.
- Participants were encouraged to stay involved and contribute actively to upcoming activities, as the project progresses toward concrete outcomes.

12. Important Reflections from the participants of the EU WS

- "We must not only transpose directives but transform them into effective national practices."
- "Cross-border resilience depends on cross-border understanding."
- "Workshops like this help us move from theory to action."
- "Learning from each other is the most efficient resilience strategy."
- "There is no resilience without cooperation."

13. Action Points & Recommendations

- Support the alignment of national legislation with EU-level resilience directives (NIS2, CER, etc.)
- Create a pan-European repository of lessons learned and good practices.
- Develop sector-specific implementation guides and maturity models.
- Continue roundtable discussions and thematic working sessions throughout the project lifecycle.
- Strengthen permanent communication channels across resilience stakeholders.
- Organize follow-up simulation and training events to test proposed strategies.