DIGITALIZATION

DOUBLE MATERIALITY	SUSTAINABILITY PLAN PILLAR	SUSTAINABLE DEVELOPMENT GOALS (SDGs)
MATERIAL TOPICS: • Digital transformation	GROWTH ACCELERATORS • Digitalization	4 QUALITY EDUCATION 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE 12 RESPONSIBLE CONSUMPTION AND PRODUCTION 13 CLIMATE ACTION

As cyber threats increase in sophistication, frequency and impact, Enel continues to act with an integrated approach, leveraging people, technologies and processes to reduce the cyber risk. Enel is also continuing its actions to reduce CO_2 emissions by reducing printed pages, monitoring PC, laptop and monitor power consumption outside normal working hours, and optimizing the use and size of digital platforms to reduce the environmental impact.

Below the 2023 results related to the previous 2023-2025 Sustainability Plan, the resulting progress and targets of the 2024-2026 Sustainability Plan, which may be redefined, added, or outdated with respect to the previous Plan.

ACTIVITIES	2023 RESULTS		2024-2026 TARGETS		MAIN SDGs
CYBER SECURITY					
Execution of cyber exercises involving plants/industrial sites	**67** cyber exercises performed	✓	**155** cyber exercises over the period 2024-2026[1]	↺	4 9
Cyber security verification actions (Ethical Hacking, Vulnerability Assessment, etc.)	**1,861** verification actions carried out	✓	**3,600** verification actions in the period 2024-2026[1]	↺	9
Disseminating the information security culture and changing people's behavior in order to reduce risks	**19** cyber security knowledge-sharing events held per year	✓	**45** cyber security knowledge-sharing events in the period 2024-2026		4 9
DIGITAL SOLUTIONS					
Activities to reduce CO_2 emissions	**-54.5 mil** printed pages (*vs* 2019)	✓	**-17 mil** printed pages in 2026 (*vs* 2019)		12 13
	6.9 mil meetings held via video-conferencing services	→	Extended use of video communication systems		12 13
	16.4 mil hours of downtime outside normal working hours	→	Actions to reduce PC, laptop, monitor hours of downtime		12 13
	65 new e-API Digital Ecosystem interconnections	✓	**90** new e-API Digital Ecosystem interconnections in the period 2024-2026		9 12

[1] The target has been redefined for greater focus.

Goals

⊕ New ↺ Redefined ⊘ Outdated

Progress

✗ Not in line → In line ✓ Achieved

N.A. = not applicable, target not included in the 2023-2025 Sustainability Plan

DIGITALIZATION

67

CYBER EXERCISES

50 in 2022 › **+34%**

1,861

ASSURANCE CHECKS (ETHICAL HACKING, VULNERABILITY ASSESSMENT)

1,587 in 2022 › **+17.3%**

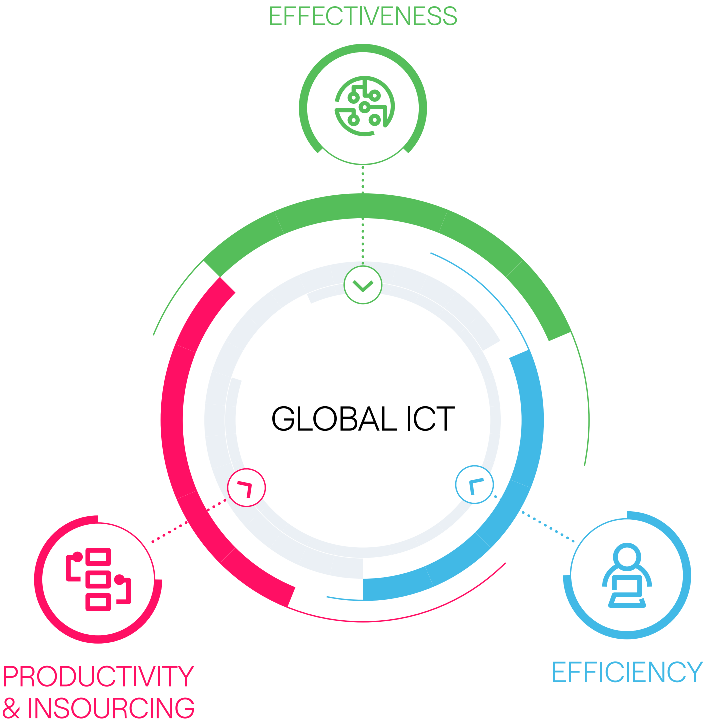
19

EVENTS TO RAISE AWARENESS OF CYBER SECURITY

19 in 2022 › **0%**

Digital transformation is a key factor for companies in the energy sector, as it can provide solutions and technologies to meet the challenges of the energy transition, optimize grid management, improve the customer experience, enable the development of renewable energy, and facilitate the work experience, ensuring high levels of service and operational efficiency. Through a new streamlined organizational and operational model, the Global Information & Communication Technology unit, within the Global Services Function, aims to:

- ensure and increase the **efficiency** of the service levels offered by Enel's digital solutions;
- increase **effectiveness** with a focus on demand management, adoption and recurring cost control processes;
- enhance **internalization**, maintaining expertise on key technologies through insourcing plans, increased training and tools to increase productivity.



Sustainable digital transformation

Digital technologies such as artificial intelligence, big data, IoT and the cloud can generate major benefits in terms of streamlining business processes, but attention must also be paid to the impact they can have on the environment and people. To achieve sustainable progress, Enel's digital transformation therefore aims to use digital solutions based on specific sustainability criteria. For this reason, the **main lines of action in 2023** addressed:

- **decarbonization** and reduction of emissions linked to digital solutions;
- **circularity** of the digital devices and materials comprising the digital assets of the Group;
- promotion of **social inclusion** through the development of assistive technologies and solutions that ensure accessibility and generate value by meeting local needs;
- promotion of **best environmental performance** and adoption of **human rights principles** with the suppliers of digital products and solutions.

Enel is also a promoter in Italy – together with the Foundation for Digital Sustainability – of the first **UNI/PdR 147:2023 Reference Practice** which sets out the requirements and guidelines for more sustainable and inclusive by-design digital technology. The Practice identifies 58 sustainability indicators, which apply to all stages of the life cycle of a digital transformation project: from initiation through to planning, execution and monitoring. The indicators are tied to the Sustainable Development Goals (SDGs) to understand the extent to which a given digital transformation project is able to harness the full potential of digital technology, while meeting the economic, social and environmental sustainability criteria. In particular, Enel has globally applied the Practice to the project of digitizing meters for energy withdrawn and fed into the grid. This highlights the strength of the goals of innovation (SDG 9), responsible consumption and economic growth through software reuse (SDGs 8 and 12), while the gender equality of the predominantly male development team emerged as a point of improvement (SDG 5). The Practice was also applied to the Data Governance project for the development of a search engine to easily find active contract documents thanks to a series of filters on contract metadata (contract date, supplier, products/services, etc.). The strengths of the project include: the goals of innovation (SDG 9), knowledge sharing within the business community (SDGs 4 and 11), and good balance in terms of the working hours needed for development activities (SDGs 3 and 8); whereas the goal to enhance the use of information, which is still not widely shared (SDG 12), emerged as a point for improvement.

Lastly, in 2023 Enel globally launched a project to **assess the ethical risk in the Group's use of artificial intelligence**, in line with the requirements of new regulations at European level (AI Act). The project highlighted the need to manage the design of digital solutions based on a methodology to identify the risks, social implications and impact of technologies, and to develop a compliance-by-design model to define the most appropriate mitigation strategies for the identified risks. As a result, a "recommendations" document was drafted for the Group, containing the points to consider when designing new digital solutions.

Inclusiveness of web portals to create value

Enel has developed a model to assess the web portals available to customers and colleagues in terms of digital inclusiveness, taking into account the social, environmental and economic sustainability impacts. The Inclusive Web Portal© framework was codified through copyright in 2023; it identifies 89 requirements, with user experience and digital accessibility as key elements, which aim to ensure digital inclusiveness. The framework highlights persistent diversity, as well as different abilities of circumstance, demographics, economic, labor, cultural, linguistic, ethnic, and gender identity diversity. The model makes it possible to identify the actions to be taken to promote a digitally inclusive environment that can create value and meet the needs of all stakeholders, so that no one is left behind in the digital transformation process.

Key drivers of the digital transformation

Circular transition of the digital value chain

Digital devices are made up of materials that, if not managed properly, can be harmful to the environment when disposed of. Enel therefore implements a Group-level strategy to reduce risks and seize the opportunities arising from the management of digital devices. Incoming and outgoing commodity flows are analyzed to establish the planning requirements and assess the risks and impacts of digital assets in terms of circularity. This analysis made it possible to identify the main critical materials present in the computers and monitors in the Company fleet (iron, copper, aluminum, and steel) and plan for the quantities of critical materials needed by Enel up to 2030 (for more details see the chapter on "Circular economy").

Enhancing digital devices through reuse and recycling

The process of decommissioning Company equipment results in the production of waste materials that require careful disposal methods. For this reason, the circular management of digital assets in the Group's various countries is achieved by helping to extend the useful life of the devices, either through sale to employees and third parties or donation to third sector entities, subject to a specific Group procedure to promote reuse and, in turn, digital inclusion (17,880 devices sold in 2023 and 38 donated). As an alternative, the Company promotes recycling of these devices (22 tons of recycled devices in 2023) which, being categorized as e-waste, are disposed of at suppliers who purchase the devices and then recycle them.

Data enhancement through sharing

The shift from monolithic architectures and data silos to systemic, distributed and enterprise-wide models means that information can achieve greater scalability, quality and speed of movement within an organization. Specifically, the e-API (Enel Application Programming Interface) ecosystem is the digital environment, consisting of software interfaces, through which all Group companies can quickly share information in real time that would normally remain confined to specific vertical applications (information silos). This ecosystem has helped speed up the adoption of digital solutions, reduce data redundancies within the Group and, more generally, reduce the amount of time and resources spent on exchanging flows of information. In 2023, 65 new e-API interconnections to the Group's applications were made, avoiding additional software development costs.

Environmental impact of digital solutions

Digital technologies can help combat climate change and help towards the energy transition by providing solutions geared toward energy efficiency and decarbonization; at the same time however, the same technologies generate emissions that negatively impact the environment. Enel's Digital Carbon Footprint Framework©, codified through copyright in 2023, made it possible to quantify the emissions produced by the digital solutions in use throughout the Group. In turn, an action plan was drawn up geared toward containing and reducing emissions through practices of optimizing cloud sizing, increasing the renewable power supply of digital infrastructure, and green coding – a software development mode that aims to limit the energy consumption required to execute algorithms. This led to a 36% reduction in CO_2 emissions from digital sources as of 2023 compared to 2018, a 206% increase in the processing capacity of the Group's systems, and a 90% increase in data storage capacity.

Digital for people

Awareness for digital sustainability

A global internal communication campaign was carried out in 2023 entitled "Sustainability by/in digital", which aimed to share a culture of digital sustainability among Enel people, make known the impacts of digital behaviors on the environment in terms of energy consumption and emissions generated, and raise awareness on the conscious use of digital technologies. The interactive campaign included the global publication of 3 news items on the corporate intranet, which covered: the first UNI/PdR 147:2023 Reference Practice, which sets out requirements and guidelines for more sustainable and inclusive digital technology; the decalogue of actions to be implemented to reduce the environmental impact of digital technology; and the guide on how to use new digital technologies while limiting energy consumption and emissions. The news items were accompanied by newsletters and surveys inviting Enel people to test their knowledge on digital sustainability issues.

Digital accessibility for inclusion of vulnerable colleagues and customers

Assistive technologies play a key role in enabling the inclusion and social participation of people with vulnerable conditions, enabling them to overcome functional issues and reduce dependence on third parties. For this reason, Enel has drawn up a catalog of assistive hardware and software where Group people can obtain immediate technical support through dedicated teams. Examples include Jaws, a screen-reading program with speech synthesis for blind colleagues; Zoom text, which lets visually impaired colleagues zoom in on any on-screen application and change the colors and shape of the mouse cursor; and Pedius, which enables deaf colleagues to communicate through speech synthesis and speech recognition technologies so that the user can use their natural voice or write. Lastly, Veasyt is a professional sign language video interpreting service (via web or app) for events and training.

Virtual meetings

- **6.9 million** meetings
- **552,800 tons** of CO_2 avoided

Printing service

- **81 million** printed pages
- **6.4 tons** of CO_2 produced

The printing service, which uses new generation printer models for better eco-sustainability, continues to be in operation at all Group offices. With a more rational use of printing thanks to increased awareness and document digitalization, this system has enabled a reduction in paper consumption over the years and, in turn, a lower impact on the environment.

Services such as instant messaging (chat) and audio/video-conferencing take full advantage of the sharing model which, through the internet, allows content to be shared and enjoyed in real time from personal computers, smartphones or tablets, thereby reducing the need to travel and, in turn, lowering carbon dioxide emissions.

PC Power Management Italy

- **16.4 million** hours of non-use
- **35.1 tons** of CO_2 produced

In 2023, monitoring continued of electricity consumption outside normal working hours linked to the IT workstations (desktop computers, laptops, monitors) of Enel people working in Italy. This was measured thanks to a Microsoft function (System Center Configuration Manager) on the workstations, which can identify when a workstation is on and not being used. Compared to previous years, idle hours have increased due to the expanded scope of devices analyzed. Nevertheless, there is a steady decrease in emissions thanks to the higher energy performance of the new PCs acquired in 2023.

Towards cyber-safe electrification

In the era of digital transformation, **cyber security** assumes a key role in ensuring the normal operation of businesses, including in view of the significant increase in cyber attacks as well as their level of sophistication and impact.

Industry studies confirm that, in line with the trend of previous years, the perception of cyber risk is growing steadily, despite the fact that previous years have been strongly characterized by conflicts and geopolitical tensions. National security agencies have therefore warned public and private institutions of potential cyber threats against critical infrastructure, often generated by activists from national and international organizations. Over the last few years, many of the world's major attacks have been carried out by leveraging the supply chain and through compromised third parties, which allowed attackers to target the primary target's customers, partners and suppliers. This caused a sharp rise in the number of victims and attacks went increasingly undetected (the so-called "scale effect"). It is also seen how the vulnerabilities detected in commonly used software products are continuously increasing and how they are taken advantage of with greater speed by IT criminals. In particular, the "zero-day" type vulnerabilities represent a large risk because they are exploited by cyber criminals to carry out attacks before software developers become aware of them and before they can release a corrective update (patch).

With reference to the energy sector, the majority of cyber attacks include ransomware, an increasingly used method that causes the exfiltration (unauthorized copy, transfer or recovery) of the victim's data and its encryption, which gives the people responsible for the attack an additional lever for receiving payment of ransom. Along with this type, 2023 saw an increase in social engineering attacks, the first step performed by cyber criminals before launching the full-fledged attack. This type leverages the victim's difficulties in recognizing the attack, exploiting emotions such as fear and a sense of urgency to push them into performing a certain action (*e.g.*, send money, divulge sensitive information, or share login credentials). Furthermore, market analysis and studies affirm that there is a high probability of an increase in cyber threats over the following few years due to an increasingly intensive use of generative Artificial Intelligence on the part of cyber criminals to refine attack techniques by successfully exploiting weaknesses linked to the human factor.

The global increase in cyber threats therefore constitutes an important rick factor for the Group, in that cyber attacks could cause errors in the normal performance of corporate processes, with consequent inefficiencies, losses of customers, interruptions in power generation and of business in general. In such circumstances, the Group may not be able to conduct its normal operations in an effective manner.
To these challenges can be added the development of the regulatory landscape concerning cyber security, which has led to the definition of complex and at times non-converging complex security requirements. Indeed, although regulations address the same objectives, they define different formalities, deadlines and time frames, making the necessary operations costly and complex.

In a similar context, for several years already **Enel** has adopted a strategic and integrated approach to the management of cyber risks. More specifically, a number of initiatives acting on the human factor (*e.g.,* awareness campaigns and simulated phishing initiatives acting), through the implementation of technical protection solutions (*e.g.,* antivirus, antispam, and multifactor authentication systems), and for the diffusion of cyber security principles into corporate processes (*e.g.,* power plant design and maintenance, customer management and procurement) have been implemented.

Policies and management models

In line with the needs of the energy industry, the Group has adopted a systemic vision of cyber security issues, as well as a global strategy of analysis, prevention and management of cyber security events.
Since September 2016, a **Cyber Security** unit was established in the Global Information and Communication Technology (GICT) Function reporting directly to the Chief Information Officer (CIO) and whose manager has the role of Group Chief Information Security Officer (CISO). The unit is committed to ensuring the governance, direction and control of cyber security issues, establishing strategy, policies and guidelines in compliance with national and international regulations, engineering support for the protection of the Group's environments, monitoring of the risk posture through checks based on processes and technology, as well as monitoring and implementing compliance requirements tied to cyber security regulations, and adopting technical solutions and procedures to mitigate any weaknesses detected. The unit works in synergy with the Business Lines and with the technical

units responsible for system design and management, thanks to the Cyber Security Risk Managers and Cyber Security Response Managers. A valid approach to cyber risk management must also attribute responsibility to the Business Lines, facilitating well-grounded decisions on the management and posture of the risk. CISO and the Cyber Security Risk Managers also make up the Cyber Risks Operating Committee, which aims to evaluate cyber risks across the business and determine the risk acceptance criteria based on the Group's risk posture. The Cyber Security Committee, chaired by the Group's CEO and made up of his/her front lines, approves the cyber security strategy and periodically (at least annually) checks its progress. In 2023, the Committee met once in July and for 2024 regular meetings are planned to bring the strategy forward. All areas participate actively in implementing the cyber security strategy by way of an integrated operating plan in line with the Group's objectives. Moreover, the cyber risk and the cyber security strategy and related initiatives are the subject matter of constant in-depth analysis on the part of the main executive bodies (*e.g.*, the Board of Directors, the Control and Risk Committee, the Board of Statutory Auditors, Supervisory Authorities, etc.) for all the legal entities and countries where the Group is present.

Moreover, the Group policy adopted in 2017 (the "**Cyber Security Framework**") addresses the principles and operational processes that support a global strategy of risk analysis, prevention and management. Based on a "systemic" vision, this Framework applies across the more traditional Information Technology (**IT**) sector, as well as to Operational Technology (**OT**) environments tied to the industrial world and the Internet of Things (**IoT**). In applying this framework, the Cyber Security Risk Management method was also established. The method is applicable to all IT, OT and IoT environments and includes all of the phases required to carry out a risk analysis and define the related mitigation plan, in line with the stated cyber security goals. To balance the advantages obtained from the operation and use of IT/OT/IoT systems with the risk that can potentially derive from them, well-informed, risk-based decisions are of fundamental importance.

Enel has also created a "**Cyber Emergency Readiness Team**" (CERT) to ensure proactive management and responses to cyber incidents, while encouraging collaboration and exchanges of information within a network of accredited international partners. Having entered into an agreement with the US national CERT, there are now 9 accreditations with Romania, Italy, Chile, Argentina, Peru, Colombia, Brazil, Spain and the USA. The Group's CERT is also part of Trusted Introducer, a service that includes 508 CERTs in 75 countries. In September 2018, Enel also joined FIRST (Forum of Incident Response and Security Teams), the largest and most widespread community in the sector, with 710 members spread across 106 countries. The operational model of CERT H24 7/7 consists of an in-house team of security analysts working in shifts. This team is dedicated completely to the protection of the Company from cyber security threats.

Definition of the IT security strategy

The cyber security strategy defines the objectives and priorities to direct and coordinate investment initiatives for the Group as a whole, and to ensure adherence to cyber security policies, setting targets, management reporting, and constant monitoring of ongoing security activities.

This process is guided by CISO and uses close integration and synergy with the various business areas, which communicate their needs, analyze opportunities, manage any criticalities, and make proposals for initiatives.

Devising strategies is an iterative activity based on sharing and consolidation of the Group's risk posture target. The various actors involved analyze the options and potential initiatives within their respective business areas in order to assess the feasibility and guarantee consensus and the necessary funds. The Cyber Security unit guides the process and, together with the other key players, gradually consolidates aspects such as future scenario, objectives and possible strategic initiatives in a cyber security strategy proposal document, with a high-level budget estimate and prioritization.

Cyber security incident management

The multiplicity and complexity of the areas in which the Group operates (data, industry and people) and of the technological components (*e.g.*, business critical systems such as SCADA – Supervisory Control and Data Acquisition, smart grids and smart meters) increasingly integrated into the Group's digital life, have made it necessary to configure a structured cyber security system. This leads to the need for a cyber defense model based on a systemic vision that integrates the IT sector (starting from the cloud down to the data center and mobile phone), the OT (everything concerning industrial sector, such as remote control of power plants) and the IoT (extension of communication and Artificial Intelligence to the world of things).

Through the monitoring systems, CERT collects 5 billion events every day relating to the Company's assets from 5 thousand data sources, correlates them through automatic analysis and on average produces daily 300 "incidents". These incidents are classified based on the Enel Cyber Impact Matrix (on a scale of 0 to 4), making use of the best events correlation capabilities thanks to the adoption of highly advanced services.

The vast majority of "incidents" are classified as **0/1**. These have no significant impact on Group systems and are automatically or semi-automatically blocked and/or managed by the existing Company defenses. In this way they are able to prevent and/or mitigate the impact of potential cyber-attacks. Incidents classified as **2/3/4** have a potential impact on the Group and are managed by CERT analysts, involving any stakeholders affected. Thanks to the protection services, each day in 2023 **CERT blocked on average 1.1 million at risk emails, 46 viruses, 206 web portal attacks, and 1.6 million connections to harmful websites**.

During 2023 Enel's CERT replied to **48 cyber security incidents with impact level 2; 2 incidents with impact level 3; and 0 incidents with impact level 4, the highest one**.

In the cases detected, to ensure an efficient and rapid response and minimize the impact on people, services and assets, all the relevant management procedures have been put in place. Specifically, when a cyber security incident becomes a potential data breach, the necessary actions are taken immediately, in line with the Enel Group "**Data Breach Management**" policy. Should a crisis situation arise that threatens the Group's business continuity, assets, reputation and/or profitability, the appropriate actions are taken immediately, in line with the specific Group policy on "Critical events management".

Moreover, the "**IT Service Continuity Management**" policy formalizes a process to bring the risk affecting the availability of IT infrastructure down to an acceptable level, support business continuity requirements, and restore IT services based on the results deriving from a Business Impact Analysis when a severe interruption occurs, including when it is caused by an accident.

Below are given the details for the number of cyber security events recorded in 2023.

	2023
Total number of cyber security breaches or other cyber security incidents[1]	**0**
Total number of customers, consumers and employees impacted by data breaches affecting the Group[2]	**0**

(1) The value reported for the KPI "Total number of cyber security breaches or other cyber security incidents" refers to level 4 cyber incidents (not including possible violations deriving from "non digital" incidents).

(2) The value for the number of the KPI "Total number of customers, consumers and employees impacted by data breaches affecting the Group" concerns the number of customers, consumers and employees affected by level 4 cyber incidents.

Main projects and initiatives

All cyber security projects, programs and initiatives are designed to avoid, mitigate or remediate cyber security risks for the entire Group. As a result, all activities are managed with a risk-based approach following the security by design principle to ensure a continuous due diligence process that also includes self-assurance activities. The most notable projects are detailed below.

CYBER EXERCISES

Over the past few years, cyber exercises have become an integral part of activities aimed at **preventing, responding to and managing cyber incidents**. These are specifically periodic exercises carried out by simulating **real cyber attacks** (without impact on systems or limitation to normal operations) and involve both technical facilities and relevant businesses. The simulations performed aim to train the responsiveness of stakeholders, verify processes and technologies in the field, meet regulatory requirements and generate awareness, thereby targeting any needs for improvement of technical and/or organizational aspects. Simulations are at all times followed by an assessment that aims to analyze their outcomes, from a quantitative and qualitative point of view, providing possible "**lessons learned**" insights where necessary. During 2023, **67 cyber exercises** were carried out globally. This confirms the extent to which this activity has become an established practice in the Group.

CYBER SECURITY GLOBAL REGULATORY COMPLIANCE

In recent years, there has been **an evolution of the legal and regulatory landscape in cyber security**, including in terms of the complexity of regulations. The latter require cross-cutting fulfillments and at the same time improvements in governance, technical-specific requirements, periodic audits, critical event notifications, and constraints and provisions in the procurement of goods and services, with continuous verification and adjustment processes over time.
To handle this complexity and streamline initiatives to **achieve compliance in the area of critical infrastructure** in the countries where the Group is present, Enel has designed and managed a **structured program** to **analyze**, **adapt** and **monitor globally** the **regulatory requirements of different compliance**, ensuring and increasingly involving the Business Lines. The program has identified **common global processes and tools**, which have been implemented to meet both the common requirements of all compliance issues and the specifics of local regulations.
To support this process, an information system named, the "**Cyber Security Global Regulatory Compliance Scheme**", has been designed and implemented to analyze the numerous regulatory requirements with respect to the Group's Cyber Security Framework, identifying any gaps there may be both at the individual country regulatory level and at Group level.
With such a tool, it is possible to effectively and efficiently identify compliance measures to be managed and monitored in the Cyber Security Regulatory Compliance program.

PLAYBOOK ISO27001 – CERTIFICATION TO ISO STANDARD

Enel has seized on the growing interest in the market for **ISO 27001 Information Security Certification**. Indeed, it has initiated certification paths to this ISO standard by achieving it already for several Legal Entities. Specifically, **Enel X**, **Enel X Way**, **Gridspertise**, **Enel Grids** and **Enel Global Services** have achieved an important milestone for the Group's cyber security by obtaining ISO 27001 certification. This important achievement certifies the information security management system for **core processes**, with a view to delivering trusted products and services to customers. Given the Group's complexity, beginning from the experiences gained in leading the path to certification to ISO 27001 standard of the Group's various Legal Entities, a **digital management tool** was designed that makes the achievement of certification **efficient, repeatable, scalable and sustainable**. The tool, called the **ISO 27001 Playbook**, achieves an **operational benchmark for the Group**, indicating key information to be prepared during certification and providing a map of Group requirements and processes. Specifically, the Playbook also equips Legal Entities with a map of manager references and evidence of the Group's cross-cutting processes, enhancing and optimizing both the specificities of the Business Lines and the effort of the Global Areas that serve the Group. transversally.

Collaborations with external bodies and agencies

The network of relations with external entities and organizations is a key element in the cyber security strategy, to share best practices and operational models, develop and strengthen information sharing channels, and help establish standards and regulations. Feedback was provided during 2023 to promote the standardization of the current cyber security regulatory landscape and the adoption of a risk-based approach and the principle of security by design. This is in view of the difficulties in managing cyber security regulations globally, which are characterized by great heterogeneity in security requirements and methods of implementation. Taking into account the context of regulatory compliance, **no cases of non-compliance with standards or cyber security regulations were detected in 2023**.

In recent years, a solid network has been established and developed by interacting with key stakeholders in the energy sector such as ANEEL (Agência Nacional de Energia Elétrica) and ONS (Operador Nacional do Sistema Elétrico) in Brazil and CNO (Consejo Nacional de Operación) in Colombia. In 2023, the Group represented **Eurelectric** to support the European Commission in the harmonization of cyber security legislation and standards within the Energy and Critical Infrastructure sector.

In Italy, a communication channel has also been established with the **Agenzia per la Cybersicurezza Nazionale ACN** (Agency for national cybersecurity) to address cyber security challenges. More specifically, Enel is among the four **pilot companies** that have participated in the project aimed at the implementation of the **Hyper SOC** (Security Operations Center), *e.g.*, an infrastructure for the collection, correlation and analysis of events of interest, with the goal of rapidly identifying emerging threats and coordinating responses to deal with them effectively. As a result of this initiative, the first achievement was the activation of the real-time information interchange portal with the ACN to intercept possible complex attack patterns at an early stage.

In addition, thanks to cooperation with other external partners, the **Cyber Harbour** was inaugurated. This is an innovation center that brings together cyber security experts, companies, investors and academia to foster the realization of innovative and competitive projects in the field of cyber security for the benefit of Italy's economic and political system.

In addition, Enel has participated in World Economic Forum working groups and contributed in recent years to the publication of several reports, including "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", "Cyber Resilience in the Electricity Industry: Analysis and Recommendations on Regulatory Practices for the Public and Private Sectors" and "Cyber Resilience in the Electricity Industry: Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector".

Training and information

The **"Cyber Security Awareness Program**" has become a constant and ongoing initiative at Group level. It is used to disseminate a cyber security culture and raise awareness of threats and attacks that exploit the human vector. Indeed, this program contributes to digitalization, in that it creates a culture of IT security, changes the behavior of people in order to reduce the cyber risk, develops technical IT security skills and makes people the first line of Company defense against cyber attacks. It uses various communication channels and dissemination tools, including both communication campaigns as well as dedicated training initiatives for clusters of people. Specifically, 19 knowledge sharing events were held in 2023 on a Global level on the issues of cyber security and various initiatives were also held at local level to disseminate and increase the culture of cyber security, with the objective of changing people's behavior so as to reduce cyber risks.

Awareness initiatives were executed through "TheRedPill", the unique Group-wide platform through which the "People Cyber Empowerment Journey" program (consisting of simulated phishing campaigns and awareness modules) is executed.

"THEREDPILL"

In 2023, cyber security awareness initiatives were continued globally through the Group's awareness platform "**TheRedPill**". The aim of this platform is to generate and enhance awareness of key cyber issues, address any upskilling and reskilling needs, and teach people how to defend themselves against cyber attacks. In particular, **simulated phishing campaigns** (8 in 2023) proceeded targeting the entire Enel corporate population and 19 **events were held to spread the culture of cyber security**. Within the "People Cyber Empowerment Journey" awareness program, launched in 2022, all of the 12 awareness campaigns planned were defined and launched.

Specific initiatives were also launched for **new hires**, with the goal of promoting cyber security awareness from the early days of employment. These include the "**Cyber Security Essentials**" course, designed to provide the knowledge needed to address cyber security challenges and promote digital awareness, an **Anti-Phishing Module** to recognize possible e-mails with malicious content, and the inclusion of specific contents related to cyber security in the Company's "**Welcome Book**".