UNIVERSITY OF PIRAEUS

School of Information and Communication Technologies
Department of Digital Systems | Postgraduate Program
M.Sc. in “Digital Systems Security”

Cybersecurity and Business Continuity in Electricity Critical Infrastructures: A Post-NIS 2 Framework Desk Research

Elisavet Konstantopoulou[1]

[1]mte2212 – Department of Digital Systems, University of Piraeus

* *Correspondence to eliskonstantopoulou@ssl-unipi.gr*

Supervisor: Prof. Stefanos Gritzalis

March 2024

Abstract

In the wake of the NIS 2 directive, which significantly elevated the cybersecurity requirements for critical infrastructures and expanded its scope to include more sectors, this thesis explores the evolving landscape of business continuity. It examines the challenges faced by organizations responsible for electricity services in maintaining uninterrupted operations while combating increasingly sophisticated cyber threats and presents a desk research framework for successful continuity implementation.

Keywords: critical infrastructure, energy, electricity, business continuity, business continuity management, business continuity management system, NIS, NIS 2, framework, desk research

"If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it."
Edward Aloysius Murphy Jr.

Contents

1 Introduction

In an era where the vitality of energy infrastructure is inextricably linked to national security, economic stability, and public safety, the importance of a robust and resilient framework cannot be overstated. The energy sector, characterized by its complex and interconnected systems, stands at the forefront of critical infrastructures vulnerable to disruptions - be they from natural disasters, technical failures, or, increasingly sophisticated cyber threats. These threats underscore the necessity for an all-encompassing business continuity approach, ensuring uninterrupted service delivery and safeguarding against potential threat instigators.

The introduction of the NIS 2 Directive marks a pivotal shift in the cybersecurity landscape for critical infrastructures, since it not only intensifies the cybersecurity requirements but also broadens its scope, compelling organizations to reassess and strengthen their resilience strategies. NIS 2, in essence, sets a new benchmark for cybersecurity and business continuity practices, more specifically incident management, reporting, and information sharing, mandating a more rigorous and standardized approach to crisis preparedness and handling. By bridging the gap between theoretical concepts and practical implementation, this master thesis endeavours to chart a course for a post-NIS 2 era, where cybersecurity and business continuity are not merely regulatory requirements, but cornerstones of a resilient energy sector.

2 Acknowledgements

I would like to express my sincere gratitude to my supervisor, Prof. Stefano Gritzali, who helped me initiate this endeavour and provided me with invaluable guidance and insightful critiques which refined this master thesis to its current form. I would, also, like to extend my gratitude to my colleagues Vasili Manousopoulo, Ernesto Zagkli, and Yanni Krasonikolaki for their generous support and insights; their willingness to share their knowledge and perspectives has significantly shaped the development of this thesis.

Last, but certainly not least, I would not hope to end this section without thanking my parents. Their unwavering support and trust have been the bedrock of my grit, and their enduring belief in me has propelled me forward, even in the face of this unprecedented academic challenge.

3 NIS 2

3.1 The Precursor: the NIS Directive

Cyber-attacks, besides being among the fastest-growing form of crime worldwide, are also growing in scale and sophistication; the rankings of the ENISA Threat Landscape reports of the last six years (2018-2023[1]) being dominated by them serving as an indication of this claim (see Table 1). The 2016 European Directive on the Security of Network and Information Systems, hereafter referred to as the 'NIS directive', established measures to ensure a high level of security across network and information systems within the EU.

Scope

One of the three pillars of the NIS directive is the implementation of risk management and reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSPs). Annex II and Annex III of the NIS directive identify the following categories of operators/sectors as OES and DSPs respectively:

- **OES:** energy (electricity, oil and gas), transport (air, rail, water and road), banking, financial market infrastructures, health, drinking water supply and distribution, digital infrastructure.
- **DSPs:** online marketplaces, online search engines, cloud computing services.

More specifically, the NIS directive establishes cybersecurity obligations for OES and DSPs, mandating them to adopt technical and organizational measures to manage risks and secure their network and information systems. These measures, aligned with the current state of the art, aim to mitigate risks and ensure service continuity by minimizing the impact of security incidents, broadly defined as events adversely affecting network and information system security. Moreover, entities are required to promptly report significant incidents to competent authorities or Computer Security Incident Response Teams (CSIRTs), including details that could help assess the incident's cross-border effects, which is something that promotes collaboration between private and public sectors, contributing to cyber defence efforts by enabling authorities and CSIRTs to respond effectively, especially when incidents have transnational implications. Shared incident data, processed and distributed within the CSIRTs network and to the public in an aggregated, anonymized form, enhances operational cooperation and cyber resilience awareness. Additionally, the NIS directive empowers competent authorities to demand information from operators for security assessment purposes, including security policies and audit results, and to issue binding instructions to address identified security deficiencies.

[1] [5], [6], [14], [34], [35]

Rank	**2018**	**2019-2020**	**2021**	**2022**	**2023**
1	malware	malware	ransomware	ransomware	ransomware
2	web-based attacks	web-based attacks	malware	malware	DDoS
3	web app. attacks	phishing	cryptojacking	social engineering threats	threats against data
4	phishing	web application attacks	e-mail threats	threats against data	malware
5	DoS	spam	threats against data	threats against availability: DoS	social engineering
6	spam	DoS	threats against availability & integrity	threats against availability: internet threats	information manipulation
7	botnets	identity theft	disinformation misinformation	disinformation misinformation	web threats
8	data breaches	data breaches	non-malicious threats	supply-chain attacks	supply-chain attacks
9	insider threats	insider threats	supply-chain attacks	N/A	zero-days
10	physical threats	botnets	N/A	N/A	N/A
11	information leakages	physical threats	N/A	N/A	N/A
12	identity theft	information leakages	N/A	N/A	N/A
13	cryptojacking	ransomware	N/A	N/A	N/A
14	ransomware	cyber espionage	N/A	N/A	N/A
15	cyber espionage	cryptojacking	N/A	N/A	N/A

Table 1: ENISA Threat Landscape 2018-2023

3.2 NIS 2 Directive

The NIS 2 directive originated as a response to the increasing frequency and sophistication of cyber threats faced by critical infrastructure and essential service providers in Europe. Its development took into account the lessons learned from the implementation of the previous NIS directive and the need to strengthen cyber security capabilities across member states. The NIS 2 directive aims to create a comprehensive cyber security standard that promotes collaboration, risk management, and preparedness for cyber crises.

3.2.1 Scope Expansion

NIS 2 expanded its scope to include more sectors and services as either essential or important entities:

- Providers of public electronic communications, networks or services
- Space
- Manufacturing of certain Critical Products (e.g., pharmaceuticals, medical devices, chemicals)
- Post & Courier services
- Digital Services (e.g., social networking, services platforms, data centre services)
- Waste Water & Waste Management
- Food
- Public Administration

It also expanded the context of some of the already existing sectors, namely the inclusion of new types of entities in the electricity sector (markets, production, aggregation, demand response and storage), the inclusion of hydrogen and district heating in the energy sector, the addition of EU reference labs, research and manufacturing of pharmaceuticals and medical devices in the health sector, and the inclusion of data centres, content delivery networks (CDNs), electronic communications and trust service providers in the digital infrastructure sector.

3.2.2 New Focus & Requirements

NIS 2 advances the groundwork established by its predecessor, by implementing a series of significant updates and improvements, which encompass, aside from a broader scope of application, more rigorous reporting requirements, an emphasis on securing the supply chain, managing vulnerabilities, maintaining cyber hygiene practices, and initiating peer reviews to foster better cooperation among member states.

Stricter Reporting Obligations & Security Framework

Entities now have more stringent reporting requirements thanks to the NIS 2 directive, which mandates that they notify the appropriate authorities of major cyber events right away. In order to improve cyber resilience, it also emphasizes the use of strong security frameworks, risk management techniques, incident response protocols, and business continuity planning.

Supply Chain Security

The directive emphasizes how crucial it is to evaluate and guarantee supply chain security. Organizations must assess the security policies of their third-party contractors and suppliers, set up contractual responsibilities, and put policies in place to reduce risks that arise from the supply chain. The goal of supply chain security is to thwart cyberattacks that can potentially penetrate a company through its vast network of allied companies.

Vulnerability Management

Entities must actively control vulnerabilities in their networks and information systems, which entails carrying out routine vulnerability assessments, quickly locating and resolving vulnerabilities, and putting in place efficient patch management procedures. Organizations can lower the possibility of threat actors exploiting their vulnerabilities and improve the overall security of their systems by proactively controlling them.

Core Internet Infrastructure & Cyber Hygiene

The importance of core internet infrastructure in preserving the security and stability of digital services is recognized to ensure the integrity and availability of online services by prioritizing the security of essential internet infrastructure. Another goal is to ensure proper cyber hygiene procedures. It is recommended that organizations put standards in place regarding strong passwords, frequent software updates, secure setups, and employee awareness training.

Peer Reviews for Collaboration & Knowledge Sharing

By introducing peer evaluations, the directive encourages cooperation and knowledge exchange among member states. These make it easier to evaluate the cyber security capabilities, tactics, and practices of other nations, allowing for the sharing of best practices and the identification of areas in need of development.

Considering the above requirements, we can deduce the directive's objectives; primarily, the fortification of the cyber resilience framework within member states by mandating the development and enactment of comprehensive cybersecurity policies and risk management practices. This strategic approach underscores the necessity of establishing robust incident management procedures that encompass mandatory reporting obligations and detailed response plans, thereby ensuring a structured and efficient reaction to cyber incidents. A critical component of the directive is the emphasis on business continuity planning, designed to safeguard the uninterrupted operation of essential services in the wake of a cybersecurity incident, which is complemented by the requirement for stringent supply chain security measures, obligating entities to rigorously assess and secure the cyber integrity of third-party suppliers, recognizing the interconnected nature of cybersecurity risks.

Furthermore, the directive places a significant focus on the human element of cybersecurity, advocating for the implementation of training and awareness programs aimed at equipping employees with the knowledge and skills to adhere to cybersecurity best practices. This human-centric approach is integral to fostering a culture of cybersecurity awareness across all levels of an organization. Additionally, the directive highlights the importance of asset management practices in identifying and safeguarding critical information systems and assets, thereby mitigating potential vulnerabilities within an organization's digital infrastructure.

Lastly, the directive delineates clear reporting obligations to relevant authorities, emphasizing the need for maintaining robust incident response capabilities, which ensures that incidents are promptly and effectively communicated, facilitating a coordinated response and leveraging collective expertise to address and mitigate cyber threats.

4 Literature Review

Existing literature explores the evolution of cybersecurity regulations within the European Union, focusing on the impact of the NIS directive on the energy sector, specifically on smart grids, as well as the intricate relationship between sector-specific legislation and NIS.

More specifically, Holzleitner and Reichl (2016) [21] delve into the directive's implications for the energy sector, highlighting its role in enhancing the cybersecurity posture of essential services, including those within the smart grid domain. They underscore the directive's mandate for OES and DSPs to adopt risk management practices and report significant cybersecurity incidents, which sets the stage for understanding the directive's broader implications for cybersecurity standards across various sectors.

Johnson and Wallis (2020) [30] study the implementation and ramifications of the NIS directive, focusing on its pivotal role in elevating cybersecurity standards among essential service providers. They underscore the directive's significance as an initiative by the EU to mitigate cyber threats to critical infrastructure and essential services, since by introducing mandatory cybersecurity measures, the NIS directive aimed not only to safeguard critical infrastructure from cyberattacks but also to instill a culture of risk management and incident reporting among vital service operators. This approach enhances the coordinated and effective handling of cyber incidents, thus bolstering the security and dependability of essential services. The authors' analysis highlights the directive's effectiveness in creating a foundation for national capabilities, fostering cross-border collaboration, and adopting a holistic approach to cybersecurity, significantly contributing to the fortification of Europe's cyber resilience.

Ducuing (2021) [16] explores the rule of prevalence within the NIS directive, as applied to C-ITS and offers an advanced analysis of the directive's interface with other EU legislations. This work critically examines Article 1(7) of the directive, which governs how sector-specific laws interact with the NIS framework when both impose cybersecurity obligations. Through the lens of the proposed, yet unadopted, C-ITS regulation, Ducuing identifies potential conflicts and ambiguities in the legal framework, arguing for clearer guidelines on how overlapping regulations should be navigated.

The literature further extends into the NIS 2 directive, highlighting critical discussions, changes, and implications presented in recent scholarly contributions. Dragomir (2021) [15] underscores the urgent need for enhanced cybersecurity measures against the backdrop of increasing online threats and the pivotal role of information security. The NIS 2 directive is depicted as a significant evolution from its predecessor, extending its reach by including new sectors. Emphasis is placed on the importance of proactive measures in mitigating cyber threats, highlighting the directive's potential to fortify organizational resilience against information theft and cyber-attacks, while addressing the multifaceted challenges of cybersecurity and proposing a more inclusive and stringent regulatory framework that accommodates the digital era's complexities.

Sievers (2021) [40] delves into the proposed revisions to the NIS regulatory regime, aiming to cover a wider array of entities across existing and new sectors. This shift from a discretionary to a size-based criterion for entity inclusion under the directive signifies a move towards uniformity and simplification in identifying entities subject to cybersecurity obligations. Sievers elucidates the classification of entities into "important" and "essential," detailing the obligations and supervisory frameworks associated with each category. This discourse presents the NIS 2 directive as a leap towards harmonizing cybersecurity standards, albeit acknowledging challenges in its practical application, particularly in the accurate identification and management of entities pivotal to societal and economic well-being.

Schmitz-Berndt (2023) [39] critically examines the challenges and implications of defining the reporting threshold for cybersecurity incidents under the evolving landscape of the NIS directive and the subsequent NIS 2 directive. The study delves into the complexities introduced by these directives in determining what constitutes a report-worthy cybersecurity incident, highlighting the shift towards a more inclusive approach that encompasses not only incidents that have resulted in harm but also those capable of causing substantial damage. Schmitz-Berndt's analysis underscores the pivotal role of legal and policy considerations in shaping the criteria for incident reporting, emphasizing the difficulty in achieving legal compliance amidst vague legal requirements. The paper insightfully argues for the necessity of including potential, non-materialized incidents in reporting mandates to provide a comprehensive understanding of the cybersecurity threat landscape, thereby enhancing the overall security framework within the European Union. This approach, Schmitz-Berndt posits, is crucial for preemptively addressing cybersecurity threats and fortifying the resilience of critical infrastructure against evolving digital threats.

Ferguson (2023) [19] explores the efficacy of the NIS 2 directive's risk management measures for essential and important entities within the European Union. The study addresses the directive's ability to mitigate cyberattacks, employing statutory interpretation and the cyber kill chain model for analysis. Ferguson's findings reveal a critical limitation in the directive's approach: it focuses on minimizing the impact of cyberattacks rather than preventing them. This limitation is rooted in the narrow scope of mandated cybersecurity measures, which overlook the early stages of cyberattacks, such as reconnaissance. Consequently, while the NIS 2 directive mandates certain cybersecurity practices, its effectiveness against sophisticated cyber threats is questioned, especially given the directive's lack of explicit requirements for entities to engage in proactive cybersecurity measures like threat intelligence and vulnerability scanning. Ferguson calls for future amendments to the directive that would require entities to undertake comprehensive cybersecurity measures, thereby enhancing the EU's cybersecurity framework's ability to thwart cyberattacks effectively.

The discussions encapsulated in these contributions highlight a collective stride towards strengthening Europe's cybersecurity framework, with the emergence of NIS 2 as a critical catalyst in this endeavour, promising a more robust and comprehensive approach to managing cyber risks.

5 Critical Infrastructure

5.1 Critical Infrastructure Overview

Throughout history, humans have consistently striven to fulfil their most fundamental needs, which remain remarkably consistent at their core: sustenance, shelter, and security. Millennia ago, our ancestors devoted their existence to securing these essentials through hunting, gathering, and rudimentary shelter construction. The methods and technologies have evolved drastically since then, but the essence of these primal needs endures. In the modern context, critical infrastructure serves as the contemporary manifestation of this age-old pursuit, facilitating the fulfilment of these enduring requirements; it ensures the provision of food, water, and warmth, as well as an array of other vital services that underpin our current way of life.

In today's world, the intricate tapestry of critical infrastructure extends far beyond basic survival needs, encompassing sectors such as energy, transportation, communication, and healthcare, all of which are interconnected and have evolved to meet the multifaceted demands of a globalized and technologically advanced society. The conveniences and efficiencies afforded by this infrastructure enable individuals to engage in daily routines without the constant preoccupation of sourcing these fundamental resources themselves. However, this reliance also introduces a heightened sensitivity to disruptions, whether through natural disasters or cyber threats, underscoring the imperative of safeguarding and enhancing the resilience of critical infrastructure.

The Groundwork

A preliminary definition of critical infrastructure, provided by the United States in 1996, was *"infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defence or economic security"*. Such infrastructure included telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. In the next years, the definition expanded to *"those physical and cyber-based systems essential to the minimum operations of the economy and government"*, now including infrastructures of law enforcement and internal security, foreign intelligence, foreign affairs, and national defence and services of intelligent transportation systems, continuity of government services, public health services (including prevention, surveillance, laboratory services), and personal health services (1998).

In 2004, the European Union made its initial move towards establishing a systematic method for protecting vital infrastructure, with the Council of the European Union recognizing the importance of such an effort [8]. This was primarily demonstrated through the adoption of two key documents: the Communication on Critical Infrastructure Protection in the Fight against Terrorism and the EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks. These documents underscored a collective dedication to bolstering the defences of crucial infrastructure against the threat of terrorism. In response, the European Commission introduced the European Programme for Critical Infrastructure Protection (EPCIP) and initiated the Critical Infrastructure Warning Information Network (CIWIN) to further these goals. Further expanding on this initiative, in December 2006, the European Commission issued directive EU COM(2006) 786. This directive required all EU member states to integrate the

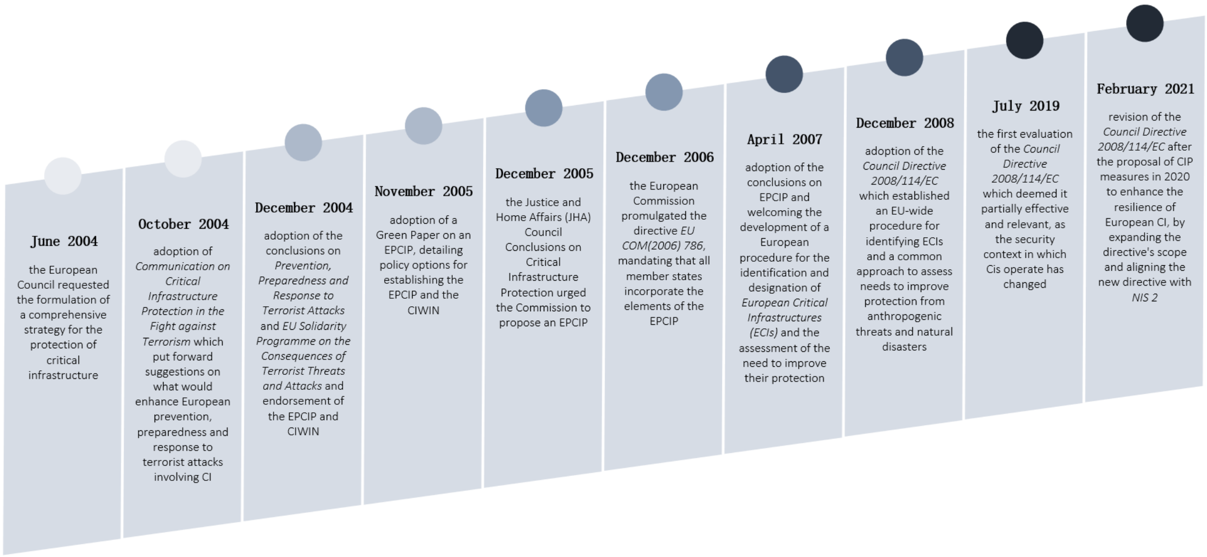

June 2004
the European Council requested the formulation of a comprehensive strategy for the protection of critical infrastructure
October 2004
adoption of *Communication on Critical Infrastructure Protection in the Fight against Terrorism* which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving CI
December 2004
adoption of the conclusions on *Prevention, Preparedness and Response to Terrorist Attacks* and *EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks* and endorsement of the EPCIP and CIWIN
November 2005
adoption of a Green Paper on an EPCIP, detailing policy options for establishing the EPCIP and the CIWIN
December 2005
the Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection urged the Commission to propose an EPCIP
December 2006
the European Commission promulgated the directive *EU COM(2006) 786*, mandating that all member states incorporate the elements of the EPCIP
April 2007
adoption of the conclusions on EPCIP and welcoming the development of a European procedure for the identification and designation of *European Critical Infrastructures (ECIs)* and the assessment of the need to improve their protection
December 2008
adoption of the *Council Directive 2008/114/EC* which established an EU-wide procedure for identifying ECIs and a common approach to assess needs to improve protection from anthropogenic threats and natural disasters
July 2019
the first evaluation of the *Council Directive 2008/114/EC* which deemed it partially effective and relevant, as the security context in which Cis operate has changed
February 2021
revision of the *Council Directive 2008/114/EC* after the proposal of CIP measures in 2020 to enhance the resilience of European CI, by expanding the directive's scope and aligning the new directive with *NIS 2*

Figure 1: Timeline of EU's journey to CI protection

principles of the EPCIP into their national laws, extending its applicability not only across the European Union but also throughout the broader European Economic Area (EEA). The EPCIP specifically identified certain assets as National Critical Infrastructure (NCI), recognizing that their disruption would have consequences confined to the affected Member State. The directive placed the responsibility for protecting these critical assets on both their owners/operators and the relevant Member State. It also encouraged each Member State to develop its own comprehensive National Critical Infrastructure Protection (CIP) programme, promoting a thorough approach to protecting infrastructure within each jurisdiction [2].

These actions were intended to enhance the resilience and security of Europe's critical infrastructure, in line with the Council's initial directives. By doing so, the European Union aimed to create a more coordinated and robust system for safeguarding essential services and facilities against potential security threats.

5.2 Critical Infrastructure Sectors

Directive 2008/114/EC identifies two main sectors: energy and transportation, each with their respective sub-sectors.

1. **Energy**: The energy sector is a cornerstone of economic stability and societal functionality, encompassing the production, transmission, and distribution of energy resources. The directive subdivides this sector into three crucial sub-sectors:

   (a) **Electricity**: this sub-sector represents the backbone of modern society, powering industries, commercial establishments, and households. It involves the generation, transmission, and distribution of electrical power. The complexity of the electrical grid and its interconnectivity render it susceptible to disruptions, necessitating robust protective measures and contingency planning.

   (b) **Oil**: central to the energy landscape, this sub-sector encompasses the production, refining, treatment, storage and transmission of oil by pipelines. Given its pivotal

[2] [9], [11]

role in fueling various sectors of the economy, the oil sub-sector's resilience is crucial. Vulnerabilities exist in its extensive supply chain, from extraction sites to refineries and distribution networks.

   (c) **Gas**: similar to oil, the gas sub-sector involves the production, refining, treatment, storage and transmission of natural gas by pipelines, as well as LNG terminals. It plays a significant role in heating and electricity generation and as a fuel source for various industries. The infrastructure, including pipelines and storage facilities, requires stringent safeguards against both physical and cyber threats.

2. **Transport**: The transport sector is fundamental to the movement of goods and people, directly impacting economic activities and societal mobility. The directive categorizes this sector into four sub-sectors, each vital for the seamless connectivity and functioning of the European Union:

   (a) **Road Transport**: this sub-sector is integral to the daily movement of people and goods. It includes the network of highways, roads, bridges, and tunnels. Ensuring the continuity and security of road transport is essential for maintaining supply chains and providing mobility.

   (b) **Rail Transport**: comprising railways, stations, and supporting infrastructure, this sub-sector is pivotal for long-distance travel and freight services. Its interconnected nature and reliance on signalling and communication systems make it crucial to safeguard against disruptions.

   (c) **Air Transport**: encompassing airports, air traffic control systems, and airlines, this sub-sector is crucial for international connectivity and commerce. The complexity and security-sensitive nature of air transport require comprehensive protective measures against a spectrum of threats.

   (d) **Inland Waterways Transport**: this sub-sector, consisting of rivers, canals, and related infrastructure, is vital for the transport of bulk goods and for its environmental advantages. The resilience of this sub-sector is critical for ensuring sustainable and efficient transport alternatives.

   (e) **Ocean, Short-Sea-Shipping and Ports**: this sub-sector is vital for international trade, connecting the European market with global partners. It includes the vast network of maritime routes, the operation of commercial vessels, and the ports that serve as hubs for international shipping and logistics. Ports not only facilitate the import and export of goods but also serve as critical junctions for multimodal transport, linking sea transport with road, rail, and inland waterways. The security and efficiency of this sub-sector are crucial, given its role in the global supply chain and its exposure to a range of potential disruptions, including geopolitical tensions, environmental challenges, and piracy. Ensuring the resilience of ocean and short-sea shipping, along with the infrastructure and operations of ports, is paramount for maintaining the continuity of trade and economic stability.

The purview of the directive is confined predominantly to the domains of energy and transport, with the explicit exclusion of the nuclear energy sector. Fundamentally, the architecture of the directive is crafted to facilitate expansion across sectors: Recital 5 elucidates that the directive is envisioned as an inaugural phase in a progressive strategy aimed at identifying and designating European Critical Infrastructures (ECIs), and posits the potential inclusion of additional sectors in subsequent iterations, contingent upon a legislative appraisal. In this context, precedence should be accorded to the Information and Communication Technology (ICT) sector, as articulated in Article 3(3) of the Directive, due to its pivotal role and intrinsic value.

The USA's Cybersecurity and Infrastructure Security Agency, on the other hand, identifies sixteen sectors.

1. **Chemical**: the sector responsible for the manufacturing, transportation, and storage of basic, pharmaceutical, consumer, and agricultural chemicals. Interdependencies can potentially span across all sectors with the most important ones being water and wastewater, transportation, communications, energy, and information technology - lifeline functions for short. The most significant risks in this sector are insider threats, cyber-attacks, natural disasters, deliberate attacks and terrorism, biohazards and pandemics.

2. **Commercial Facilities**: the sector encompassing establishments that the public uses daily to conduct business, purchase retail products, and enjoy recreational events and accommodations (e.g., hotels, casinos, amusement and theme parks, retail facilities, stadiums, and cultural properties). This sector's interdependencies include the energy, water and wastewater, emergency services, communications, transportation systems, information technology, healthcare, financial services, government facilities, and food and agriculture sectors. The most significant risks in this sector are natural disasters, armed attackers and unarmed aircraft systems, pandemics, cyber attacks, chemical, biological and radiological attacks, mass protests, theft, and supply chain disruptions.

3. **Communications**: the sector responsible for helping individuals bypass geographic distances by delivering voice, video and data services through broadcasting, cables, satellites, and wired and wireless connections. The private sector is primarily responsible for the protection of the infrastructure supporting all these capabilities, while the interdependencies span the sectors of energy, information technology, financial services, emergency services, and transportation. The most significant risks in this sector are natural disasters, supply chain vulnerabilities, global political and social implications, and cyber attacks.

4. **Critical Manufacturing**: the sector responsible for the production of primary metals, machinery, electrical equipment, components and transportation equipment. This sector's interdependencies include the energy, communications, information technology, transportation, chemical, water and wastewater sectors, as well as internal interdependencies among the critical manufacturing sub-sectors. The most significant risks in this sector are natural disasters, supply chain disruptions, global political and social implications, deliberate attacks and terrorism, and cyber-attacks.

5. **Dams**: the sector responsible for the delivery of critical water retention and control services. This sector's interdependencies include energy, communications, information technology, food and agriculture, chemical, nuclear, transportation, emergency services, and water and wastewater sectors. The most significant risks in this sector are natural

disasters, erosion and structural issues, ageing infrastructure and workforce, deliberate attacks and terrorism, and cyber-attacks.

6. **Defense Industrial Base**: the sector responsible for providing direct assistance to military operations by engaging in activities such as research and development, system design, manufacturing, integration, and the maintenance of depots, focusing on servicing military weapon systems, subsystems, components, sub-components, or parts. This sector's interdependencies include the energy, transportation, and information technology sectors, while the most significant risks in this sector are cyber threats, insider threats, phishing attacks, and bad implementation of information security practices.

7. **Emergency Services**: the sector responsible for delivering an extensive array of preventive, preparatory, responsive, and recuperative services in the course of routine operations as well as in the aftermath of incidents, which is comprised of physical, cyber and human components. This sector's interdependencies include energy, communications, information technology, transportation, water and wastewater, and healthcare and public health, as well as internal interdependencies among the emergency services themselves. The most significant risks in this sector are natural disasters, violent extremist and terrorist attacks, chemical, biological, radiological, and nuclear incidents, and cyber attacks.

8. **Energy**: the sector responsible for the production, refining, storage, and distribution of oil, gas, and electric power (excluding hydroelectric and commercial nuclear power facilities and pipelines). The interconnections of this sector extend across all critical infrastructure sectors, while the most significant risks in this sector are different for each sub-sector; electricity and oil and gas. For the former, the most prominent risks include but are not limited to, natural disasters, ageing infrastructure and workforce and cyber attacks, and for the latter natural disasters, operational hazards, terrorist activities, aging infrastructure and workforce, cyber attacks and insider threats. Naturally, the risks among the sub-sectors overlap.

9. **Financial Services**: the sector responsible for a multitude of entities, encompassing depository institutions, investment and insurance providers, various credit and financing organizations, along with essential financial utilities and services. Ranging from globally influential corporations to community banks and credit unions, the organizational and regulatory framework of this sector is contingent upon the spectrum of financial services rendered, including deposit and consumer credit products, payment systems, credit and liquidity offerings, investment products, and risk transfer products. This sector's interdependencies include the energy, communications, and information technology. The most significant risks in this sector are natural disasters, violent extremist and terrorist attacks, and cyber attacks.

10. **Food and Agriculture**: the sector responsible for the supply, production, processing, storage, transportation, and distribution of food meant for both humans and animals. This sector's interdependencies include the energy, communications, information technology, commercial facilities, financial services, transportation, and water and wastewater sectors. The most significant risks in this sector are natural disasters, diseases and pests, violent extremist and terrorist attacks, supply chain attacks, and cyber attacks.

11. **Government Facilities**: the sector responsible for overseeing and safeguarding a diverse array of properties owned or rented by federal, state, local, and tribal governments, which range from publicly accessible spaces used for business, commerce, or recreation to non-public locations holding sensitive information, materials, processes, and equipment. The sector encompasses a variety of structures such as general-use office buildings, military installations, embassies, courthouses, and national laboratories, including those that house crucial equipment, systems, networks, and functions. It also includes cyber elements like access control systems and closed-circuit television systems, as well as individuals with essential roles or possessing tactical, operational, or strategic knowledge, all contributing to the protection of sector assets. This sector's interdependencies include the energy, communications, information technology, transportation, emergency services, financial services, commercial facilities, healthcare, and water and wastewater sectors. The most significant risks in this sector are natural disasters, intentional and unintentional man-made threats (e.g., human errors and omissions, social engineering, security violations, coercion, violent extremist and terrorist attacks), pandemics, ageing infrastructure, and cyber attacks.

12. **Healthcare and Public Health**: the sector responsible for providing essential goods and services crucial to local, national, and global health security, supporting core mission areas such as prevention, protection, mitigation, response, and recovery and focusing on building community health resilience, expanding medical capacity, enhancing situational awareness, integrating capabilities into emergency management, and strengthening global health security. It spans both public and private sectors, including healthcare facilities, research centres, suppliers, and IT systems. This sector's interdependencies include the energy, transportation, communications, information technology, emergency services, and water and wastewater sectors. The most significant risks in this sector are pandemics and health crises, natural disasters, man-made threats (e.g., dissemination of biological or chemical agents, use of radiological, nuclear, or explosive devices, attacks on critical facilities by malicious actors, domestic extremist groups, or international terrorist organizations), supply chain attacks, and cyber attacks.

13. **Information Technology**: the sector responsible for providing products and services vital to the smooth operation of the global information-based society. Its functions, involving both physical assets and virtual systems, include the research and development, manufacturing, distribution, upgrades, and maintenance of IT products and services, with its interdependencies spanning across all other sectors and its most significant risks being cyber attacks, supply chain attacks, natural disasters, infrastructure failure, and potential man-made threats (e.g., attacks on critical facilities by malicious actors or human negligence).

14. **Nuclear Reactors, Materials and Waste**: the sector responsible for overseeing the safe operation, transport, and disposal of nuclear materials, while ensuring stringent regulation and security due to its potentially hazardous impact on human and environmental health and critical infrastructure. This sector's interdependencies include the energy, communications, transportation, critical manufacturing, healthcare, emergency services, chemical, and water and wastewater sectors. The most significant risks in this sector are natural

disasters, structural issues, ageing infrastructure and workforce, terrorist attacks, supply chain attacks, source diversion or mishandled and “orphan” radioactive sealed sources, and cyber attacks.

15. **Transportation Systems**: the sector responsible for ensuring a secure and resilient network across aviation, maritime, freight rail, highway, pipeline, postal, shipping, and mass transit, facilitating the smooth and safe movement of people and goods without undue disruption, fear of harm, or loss of civil liberties. This sector’s interdependencies include the majority of the other sectors, namely the chemical, communications, critical manufacturing, dams, defence industrial base, emergency services, energy, food and agriculture, information technology, and water and wastewater sectors. The most significant risks in this sector are natural disasters, violent extremist and terrorist attacks, and ageing infrastructure.

16. **Water and Wastewater Systems**: the sector responsible for ensuring the provision of safe drinking water and the proper treatment of wastewater, crucial for public health and environmental protection, and it involves a collaborative effort among various partners to enhance the sector’s security and resilience against all hazards, maintaining continuity of services vital for the nation’s health and economy. This sector’s interdependencies include the chemical, energy, food and agriculture, healthcare, transportation, dams, information technology, emergency services, and nuclear sectors. The most significant risks in this sector are natural disasters, ageing infrastructure, and cyber attacks.

As shown in Figure 2, the critical infrastructure sectors are interconnected in a complex network that, quite clearly, becomes a prime target for adversarial attacks. This is, primarily, due to the fact that these interdependencies amplify the potential attack surface since a breach in one sector can precipitate vulnerabilities and expose latent weaknesses in others, often leading to a compounded and more extensive impact. Furthermore, the pronounced ramifications that successful attacks can entail create an alluring environment, where any disruption, manipulation, or incapacitation within this domain can lead to cascading effects, impacting not just the immediate infrastructure but also have far-reaching consequences across multiple sectors, and, ultimately, various facets of societal functioning.

5.3 Energy Sector Overview

The energy sector recognized universally as a cornerstone of modern societies, plays an indispensable role in shaping national security, economic stability, and the daily lives of individuals and communities. This sector, characterized by its dynamic nature and complexity, is fundamentally involved in the production, transmission, and distribution of energy in its various forms, including electricity, oil, and gas. The strategic importance of this sector cannot be overstated, given its integral role in driving industrial growth, enabling the functionalities of the rest of the sectors, and supporting the functionalities of the daily lives of individuals.

Within the energy sector, the aforementioned sub-sectors can be identified, each with its unique set of characteristics, challenges, and infrastructure. The three primary sub-sectors, as delineated by Directive 2008/114/EC, include **electricity**, **oil**, and **gas**. The infrastructure underlying these sub-sectors consists of a network of assets deemed critical for national and regional stability; power generation facilities, refineries, pipelines, and transmission lines are

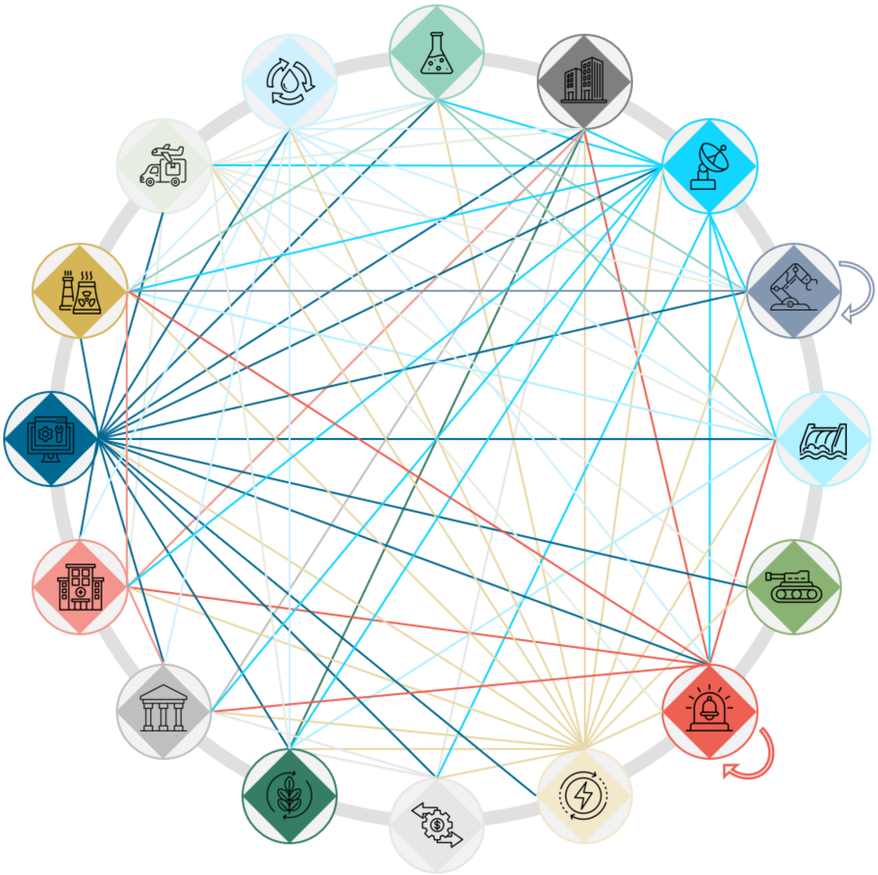


Figure 2: Diagram of interdependencies of critical infrastructure sectors

among the key assets that form the backbone of the energy sector. Their operational integrity and security are paramount, not just for the sector itself and for the overall functioning of societies and economies that rely heavily on the continuous and uninterrupted supply of energy, but also for the vital support it provides to other critical infrastructure sectors.

To delve deeper into this vast network of critical assets, we ought to delineate the following fundamental components: generation, transmission, distribution, and supply. These elements collectively form the cornerstone of the sector, each playing an integral role in ensuring the seamless operation, reliability, and sustainability of energy services [3].

1. The **production** level encompasses the initial generation or extraction of energy resources. Within the electricity sub-sector, this phase includes facilities capable of converting various primary energy sources, ranging from fossil fuels and nuclear reactions to renewable resources like hydropower, wind, and solar radiation, into electrical energy. For the gas and oil sub-sectors, production entails the extraction of hydrocarbon resources from terrestrial or marine reserves through drilling techniques. These operations are foundational, providing the initial input for the energy supply chain.

2. The **transmission** level involves the large-scale movement of energy from its production sites to distribution centres or processing facilities. In the case of electricity, this is characterized by the conveyance of high-voltage electrical power across extensive networks of transmission lines. Gas and oil transmission, conversely, relies on an intricate system of pipelines designed to transport these resources over long distances from their extraction sites to refineries or storage installations. This stage is critical for bridging the geographical gap between areas of production and regions of consumption.

3. At the **distribution** level, energy is delivered from the main transmission systems to individual consumers. In the electrical sector, this includes the step-down transformation of voltage levels for safe residential and commercial use, facilitated through a network of substations and local distribution lines. For gas and oil, this phase involves the final routing through smaller pipelines or delivery mechanisms, ensuring that these resources reach end-users efficiently and safely. This level is key in tailoring the supply to meet the specific demands of diverse consumer bases.

4. The **supply** level is concerned with the commercial aspects of energy provision, including the sale and marketing of energy products and services to end consumers. This involves utility companies and energy suppliers engaging in the administration of energy provision, customer service, and billing. Within the electricity sub-sector, suppliers offer a variety of energy plans and innovative solutions to meet consumer needs, while in the gas and oil sectors, supply services extend to the direct provision of these fuels for heating, cooking, or transportation purposes. The supply level is integral to the energy ecosystem, ensuring accessibility and choice for consumers across different sectors.

The dynamics of the energy sector are influenced by a myriad of factors including market forces, geopolitical tensions, regulatory policies, technological advancements, supply and demand fluctuations, price volatility, and the transition towards renewable energy sources, that

[3] [12], [17]

Sub-Sectors Stages	Electricity	Gas	Oil
Production	fossil fuels (coal, gas, oil, other), renewable (solar, wind, hydro, biomass, geothermal), nuclear	organic sources (biogas, biomethane), non-biological renewable sources using electricity (renewable hydrogen, synthetic methane)	extraction form the earth
Transmission	step-up transformers that increase the voltage this high-voltage electricity is transmitted through a network of electrically conductive wires of aluminium or copper these lines are called high-voltage transmission lines that can transmit electricity over long distances	pipes, compressor stations, pressure regulation facilities, meters to move and track gas (600-1200 psi)	pipelines, tankers, or trucks transport crude oil to refineries
Distribution	in an electric distribution substation the high voltage electricity from the high-voltage transmission lines is passed through step-down transformers that lower the voltage the electricity is then transmitted to a network of local electric distribution lines before electricity enters a home, the voltage is again lowered using step-down transformers	interconnects to the transmission system and then gas goes through main and line pipes that are smaller than the transmission pipes smaller compressors, valves to control flow, pressure regulators, meters (0.25-60 psi), and the SCADA system (monitor and remotely control components of the distribution system)	distribution from storage facilities to markets & end-users through pipelines, tanker trucks, maritime shipping, etc.
Supply	sale and purchase of electricity to/from the grid	sale and supply of gas to commercial, industrial, and residential users	sale of oil & oil products to various market segments

Table 2: Energy Sub-Sectors and Stages

drive the sector's dynamics. This deems the need to maintain the continuous operation of this sector imperial. Furthermore, the energy sector does not operate in isolation; its profound interdependencies with other critical sectors, such as communications, information technology, critical and other manufacturing, and healthcare, amplify the potential impact of any disruption, underscoring the need for a holistic approach to risk management and continuity planning. Adherence to standards such as ISO 22301 is essential for fortifying the sector against a range of risks and ensuring business continuity in the face of unforeseen disruptions, of which it is certainly not devoid. As the sector evolves, trends such as the shift towards renewable energy, digitization, and smart grid technologies are shaping its future trajectory. These trends, coupled with policy shifts and technological innovations, are transforming the sector, presenting both opportunities and challenges.

5.4 Electricity Sub-Sector Threat Landscape

The types of threats faced by the electricity, natural gas and oil industries vary widely, as well as the meaning of "risk" as perceived by each organization. As far as the electricity sub-sector is concerned, risks can be assessed in terms of the potential impact on the reliability of the services provided, namely the loss or interruption of electricity provision, or concerning the operational and financial security, namely the impact on the financial health and reputation of the entity in question.

As stated in section 2.2 the most prominent identified threats are:

- **Cyber and physical security threats**

The US Department of Homeland Security has acutely stated the following in its 2019 Guide to Critical Infrastructure Security and Resilience:

Critical infrastructure has long been subject to risks associated with physical threats and natural disasters and is also now increasingly exposed to cyber risks. These risks stem from a growing integration of information and communications technologies with critical infrastructure and adversaries focused on exploiting potential cyber vulnerabilities. As physical infrastructure becomes more reliant on complex cyber systems for operations, critical infrastructure can become more vulnerable to certain cyber threats, including transnational threats.

The increasing digitalization of the electricity sub-sector has heightened its vulnerability to cyber-attacks, which can disrupt operations, compromise sensitive data, and even cause physical damage to infrastructure. Physical security threats, including sabotage or terrorist attacks on critical infrastructure, pose equally grave risks [3]. These threats necessitate robust cybersecurity measures and physical security protocols to protect assets from unauthorized access and ensure the continuity of operations.

- **Natural disasters and extreme weather conditions**

  Natural disasters such as hurricanes, earthquakes, floods, and extreme weather events like heatwaves or cold snaps can cause extensive damage to electricity infrastructure facilities, especially considering the fact that a great number of electricity facilities are outdoors [7]. Such events have the potential to not only cause immediate disruption to power operation levels but also entail long-term recovery efforts, highlighting the need for disaster-resilient infrastructure and effective emergency response plans to minimize downtime and accelerate restoration efforts.

- **Workforce capability ("aging workforce") and human errors**

  The human aspect of any system is proven time and time again to be the weakest link. Coupled with the risk of human errors, which can result from both operational complexities and the lack of skilled personnel, this challenge underscores the importance of succession planning, workforce development, and the integration of automation and advanced technologies to mitigate the impact of human errors.

- **Equipment failure and aging infrastructure**

  Many components of the electricity infrastructure are ageing and are increasingly prone to failures. Such failures can lead to widespread outages and necessitate costly repairs.

- **Evolving environmental, economic, and reliability regulatory requirements**

  The electricity sector is undergoing significant changes, driven by technological advancements, shifts towards renewable energy sources, and fluctuations in fuel supplies. These changes present both opportunities and challenges, requiring adaptations in operational practices, grid integration strategies, and supply chain management to accommodate new energy sources and technologies while maintaining grid stability and reliability.

- **Changes in the technical and operational environment, including changes in fuel supply**

  The electricity sector is experiencing transformative changes in its technical and operational environment, primarily driven by advancements in technology, shifts in regulatory policies, and changes in consumer demand. These changes are further compounded by fluctuations in fuel supply, which directly impact the cost, availability, and choice of fuels used for electricity generation. The transition towards renewable energy sources, such as wind, solar, and hydro, in response to environmental concerns and policy incentives, represents a significant shift from traditional fossil fuels like coal, oil, and natural gas. This transition necessitates adjustments in grid management, energy storage solutions, and infrastructure to accommodate the variable nature of renewable energy sources.

Changes in fuel supply, whether due to geopolitical events, market fluctuations, or shifts towards sustainable energy sources, can also have profound effects on the electricity sector. These changes require flexible and adaptive strategies for fuel procurement and management, as well as investment in alternative energy sources and technologies to mitigate the risks associated with fuel supply volatility.

Cybersecurity Challenges in the Electricity Sector

A system unique to the energy sector is the Supervisory Control and Data Acquisition system, or SCADA for short [2]. It is used to control and monitor industrial processes by gathering real-time data from sensors and devices located in remote or industrial environments, allowing for the centralized monitoring and control of operations [4]. With their ability to integrate with a wide range of industrial devices and their extensive use across critical infrastructure, SCADA systems form the backbone of modern industrial automation and control, laying the groundwork for more advanced technologies like IoT integration and smart grids.

Technological innovation is a driver for development, but also the key which unlocks a door with new risks and threats waiting on the other side. The connectivity of operating environments, driven by the desire for efficiency, competitive advantage, and the capabilities of the Internet of Things (IoT), has led to an intricate web of cyber-physical systems [1]. Such systems, while enhancing productivity and capabilities, expand and steepen the attack surface due to several factors, including, but not limited to, the rising number of entry points for attackers, the added interdependencies, IoT device's inherent vulnerabilities, inadequate device management, outdated or insecure software, and potential compatibility issues with already existing infrastructure. In essence, the modernization of legacy systems - once isolated, now connected to the Internet - has created a pool of novel vulnerabilities.

The smart grid, an electrical infrastructure with technological enhancements to monitor energy use and optimize conveyance of that energy according to related needs, is another emerging technology. In contrast to conventional electrical networks that function as a one-way conduit for the delivery of electricity to consumers, smart grids facilitate information exchange between energy providers and their clientele in both directions. The reliance on and utilization of information networks render the grid vulnerable to various device and network risks. Unlike traditional power grids which were insulated from external environments like the internet, smart grids are susceptible to remote attacks that can target essential components (e.g., power generators) from numerous points within the infrastructure [32]. The operational disruption of a smart grid could lead to widespread and severe consequences, including the loss of power for homes and facilities. Key security challenges in smart grids, similar to the ones applicable to IoT, include an expansive attack surface with an array of unique vulnerabilities, the involvement of multiple stakeholders which complicates the coordination of a unified defence strategy,

[4] a more detailed analysis of the SCADA systems can be found in the Annex

and the incorporation of consumer devices into the smart grid, which introduces novel attack vectors, increasing the potential for exploiting vulnerabilities from numerous, less controllable sources.

Attacks may originate from insiders with detailed system knowledge or outsiders without direct knowledge but capable of gathering information through surveillance [13]. These threats might be deliberate, aimed at causing harm, or inadvertent, resulting from carelessness or oversight. Prominent cyber-attack types posing risks to smart grids include:

- **Denial of Service (DoS)** attacks significantly threaten smart grids by disrupting electricity availability, often through overwhelming traffic or exploiting system vulnerabilities, potentially leaving millions without power and causing extensive financial and operational damage.
- **Man-in-the-Middle** attacks interfere with communications between devices or with SCADA controllers, aiming to disrupt or alter data transmission.
- **False Data Injection** involves sending misleading information into the network, affecting the grid's operation and potentially leading to financial losses by tampering with measurement data or incurring unwarranted charges for consumers.
- **Malware** attacks, where malicious software targets smart meters or company servers, can alter functionality, steal sensitive consumer data, or spread false information.
- **Replay** attacks, where attackers reuse valid data maliciously to masquerade as legitimate senders, gaining unauthorized access to networks or imposing fraudulent charges on consumers by replicating outdated consumption messages.

Before proceeding to the next section, it must be noted that entities within the electricity sector, are recognized as critical infrastructure not only for their indispensable role in powering other sectors and sustaining societal functions but also due to the heightened risk they pose to human safety. Service disruptions, whether stemming from accidents or deliberate attacks, carry the potential for cascading effects across multiple sectors, underscoring the importance of ensuring business continuity. However, beyond the imperative of maintaining operational continuity for the "greater good," there lies an equally critical responsibility to safeguard the individuals who operate within these facilities. The fortification of entities in the electricity sector must therefore be pursued with a dual focus: ensuring the resilience and reliability of service to society at large while also prioritizing the safety and well-being of the employees. This dual focus ensures that efforts to enhance business continuity and operational resilience are balanced with the imperative to protect human lives, underscoring the sector's commitment to both societal welfare and the safety of its workforce.

6 Business Continuity

6.1 Business Continuity Frameworks

In the realm of Business Continuity, the establishment and adherence to structured frameworks are paramount for ensuring systematic preparedness and effective response to disruptions. These frameworks provide comprehensive guidelines and best practices for organizations to identify, evaluate, and manage the risks associated with unexpected incidents. In this subsection, we explore three pivotal frameworks that have been widely recognized and adopted across various sectors for their robust approach to business continuity and disaster management. Each framework brings a unique perspective and methodology, contributing significantly to the overarching goal of organizational resilience. ISO 22301, which sets global standards for Business Continuity Management Systems; NIST 800-34, a guideline pivotal for federal information systems in the United States; and NFPA 1600, a standard encompassing broader aspects of disaster and emergency management will be explored. The examination of these frameworks will provide a comprehensive understanding of the principles, practices, and strategic implications inherent in effective business continuity planning and implementation.

ISO 22301: an internationally recognized standard that delineates the requirements for establishing, implementing, operating, maintaining, and improving a Business Continuity Management System (BCMS). This standard is formulated to aid organizations in the preparation, response, and recovery from unforeseen and disruptive incidents. It provides a comprehensive framework for organizations to systematically identify potential threats, assess their impacts, and develop and manage robust plans and responses for ensuring business continuity. Applicable to organizations of all types and sizes, ISO 22301 underscores the importance of resilience and continuity in the face of diverse disruptions, thereby facilitating a structured and strategic approach to business continuity [27].

NIST 800-34: full name *Contingency Planning Guide for Federal Information Systems* is a guideline developed by the National Institute of Standards and Technology (NIST), USA. This document offers detailed directives for federal agencies and other entities on the development and maintenance of effective contingency plans for information systems. The guideline is structured to provide comprehensive insights into conducting business impact analyses, formulating recovery strategies, and establishing and maintaining contingency plans. It encompasses a broad spectrum of activities including plan development, maintenance, and testing. As a part of the NIST Special Publication 800-series, it contributes significantly to the domain of computer security and information assurance, emphasizing the importance of preparedness and resilience in information systems [38].

NFPA 1600: developed by the National Fire Protection Association, represents a standard for Disaster/Emergency Management and Business Continuity Programs. This standard offers an exhaustive framework for the development, implementation, assessment, and maintenance of disaster management and business continuity programs. Recognized and utilized by a variety of entities, including public, private, and non-governmental organizations, NFPA 1600 provides guidelines that span program management, planning, execution, and continuous improvement processes. The standard is designed to aid organizations in the effective management of a wide array of emergencies and disasters, ensuring a comprehensive and systematic approach to disaster management and business continuity [37].

Criteria \ Framework	ISO 22301	NIST 800-34	NFPA 1600
Focus	Comprehensive BCM	Contingency Planning for Federal Information Systems	Disaster/Emergency Management and BC
Scope	Global; applicable to all types of organizations	Primarily for U.S. federal agencies, but applicable broadly	Applicable to public, private & non-governmental organizations
Target Audience	Organizations of all sizes and types seeking to manage BC risks	Federal agencies & other entities managing information systems	Organizations seeking a comprehensive approach to disaster/emergency management and BC
Key Features	Identifying potential threats & impacts Guidelines for developing robust continuity plans Emphasis on resilience & adaptability	Guidelines on BIA & recovery strategies Focus on maintaining & recovering IT systems In-depth contingency planning processes	Guidelines covering a wide range of emergency management aspects Focus on integrated preparedness, response, recovery, & mitigation strategies Emphasis on program management & continuous improvement
Primary Objective	Ensure business resilience & continuity in the face of disruptions	Ensure effective recovery of information systems following disruptions	Provide a comprehensive framework for managing disasters & emergencies, along with BC
Methodology	Plan-Do-Check-Act (PDCA) cycle for continuous improvement	Structured approach to planning, implementation, & recovery of IT systems	Holistic approach to emergency management, including prevention, preparedness, response & recovery

Table 3: Business Continuity Frameworks Comparison

In this thesis, the focus will be primarily on the ISO 22301 framework for establishing and managing a Business Continuity Management System, hereafter referred to as a 'BCMS', a choice that is grounded in several key reasons. Firstly, ISO 22301 is a globally recognized standard, offering a universally applicable framework that transcends geographical and sector-specific boundaries. This universal applicability is crucial given the diverse nature of threats and disruptions faced by organizations worldwide. Secondly, the framework is comprehensive in its approach, covering all aspects of business continuity management from understanding and mitigating risks to ensuring resilience and adaptability in the face of disruptions, ensuring a holistic view of business continuity, crucial for the electricity sector's complex and interconnected environments. Moreover, ISO 22301's alignment with the Plan-Do-Check-Act cycle, hereafter referred to as the 'PDCA cycle', of ISO 27001 facilitates continuous improvement, a critical aspect for any dynamic and evolving industry like the electricity sector, as well as compatibility with the rest of the ISO standards family; in the same vein, the ISO 22313, 22317, 22318, 22330, and 27019 standards can serve as supplementary guidelines for managing business continuity, while having an ISO 27001 certified Information Security Management System, hereafter referred to as an 'ISMS', ought to be a requirement for the entities in question. Lastly, the framework's focus on proactive risk assessment and management resonates with the need for preemptive strategies in managing the unique risks associated with electricity critical infrastructures.

6.2 Building a BCMS with the ISO Standards

Business continuity ensures that an organization, given instances of disruption, can maintain its operations and achieve its business objectives while demonstrating a proactive control of risks and reducing legal and financial exposure. It is a comprehensive and strategic discipline which encompasses a systematic approach to identifying, assessing, and mitigating potential risks and threats to an enterprise's critical functions and resources. The overarching goal of business continuity is to ensure the sustained and seamless operation of essential business processes, services, and infrastructure, even in the face of unforeseen and disruptive events, such as natural disasters, technological failures, or other adverse circumstances.

The ISO 22301 standard specifies the structure and requirements for implementing and maintaining a BCMS which the organizations ought to tailor according to their legal, regulatory, organizational and industry requirements, products and services, employed processes, their size and structure, and the requirements of their interested parties. Its most vital components include a business continuity policy and the accompanying management processes as well as documented information supporting operational control and enabling performance evaluation and well-defined roles and responsibilities.

Following the PDCA cycle of ISO 27001, the standard outlines this dynamic and evolving discipline that necessitates constant review and refinement in tandem with changes in the organizational landscape, technology, and external factors that may impact an enterprise. By adopting such an approach to business continuity, organizations will be able to safeguard their reputation, maintain stakeholder confidence, and fulfil their obligations to clients, employees, and other relevant entities, thereby ensuring the sustainability and longevity of their operations in the face of adversity.

6.3 Building an ISO 22301 BCMS according to ISO 27001

The integration of the PDCA cycle, a fundamental concept from ISO 27001, into the establishment and maintenance of a BCMS as outlined in ISO 22301, offers a systematic and effective approach for organizations to enhance their resilience and response capabilities. This alignment ensures a comprehensive and adaptive strategy for managing business continuity risks. ISO 22313 is the standard which meticulously outlines this approach.

Plan Phase: Establishing a BCMS

In the **Plan** phase, the foundation of the BCMS is laid out, which involves establishing a comprehensive Business Continuity (BC) program: business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity. Key to this stage is the creation of an oversight committee, responsible for steering the BC initiatives and ensuring alignment with the organization's objectives; the development of robust policies and procedures tailored to the organization's context forms the core of this phase, as these policies will articulate the organization's commitment to business continuity and define the scope, objectives, and principles of the BCMS. Additionally, establishing a documentation system is critical, as it ensures that all BC-related information is systematically organized, accessible, and up-to-date, providing a reference point for all subsequent activities.

Do Phase: Implementing the BCMS

The **Do** phase involves putting the planned elements into action. Conducting a thorough Business Impact Analysis (BIA) and Risk Analysis (RA) is pivotal to understanding the potential impacts of disruptive incidents and to identify critical areas of focus. Based on these analyses, the development of a Disaster Recovery Plan (DRP) is essential, since it shall provide clear guidelines and procedures for restoring critical functions post-disruption. Concurrently, creating a communication plan is vital to ensure effective communication with stakeholders and the appointed professional during a crisis. Finally, exercising the program through drills and simulations is also crucial, as it helps in identifying gaps and preparing the organization for real incidents.

Check Phase: Monitoring and Reviewing the BCMS

In the **Check** phase, the organization evaluates the effectiveness of the BCMS. This involves conducting internal audits and tabletop exercises, which are instrumental in assessing the efficiency and applicability of the implemented policies, procedures, and measures. Furthermore, scheduling regular management reviews provides an opportunity for leadership to reflect on the BCMS's performance and to ensure ongoing commitment and resource allocation, as well as the authorization of remediation actions.

Act Phase: Continual Improvement of the BCMS

Finally, the **Act** phase is centred on implementing corrective measures based on the insights acquired during the Check phase, which is imperative for addressing deficiencies and enhancing the BCMS's effectiveness, while also providing an opportunity to reassess the scope of the BCMS. The continuous enhancement of these measures ensures that the BCMS maintains its effectiveness and relevance, adeptly adjusting to emerging threats, organizational changes, and the evolution of industry standards and practices.

This cycle of continuous improvement is at the heart of both ISO 27001 and ISO 22301, ensuring that the BCMS is not something static, but rather a dynamic and evolving system that enhances organizational resilience. By integrating the PDCA cycle from ISO 27001 into the BCMS framework of ISO 22301, organizations can ensure a comprehensive, structured, and adaptive approach to business continuity, significantly enhancing their ability to manage and mitigate disruptions effectively. Having delineated the fundamental steps for establishing a BCMS as per ISO 22301 and ISO 27001 in a general context, it is now imperative to delve into the practicalities and specifics of implementing these steps within the electricity sector, tailoring the available frameworks to address the unique challenges and intricacies inherent to it. Concisely, below is a condensed overview of each ISO standard to be utilized:

- **ISO 22301** specifies requirements to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. It is the premier standard for business continuity management systems and it will be used to define the core structure of the BCMS.

- **ISO 22313** provides guidance and recommendations for implementing a BCMS based on the foundational requirements established in ISO 22301. This standard offers detailed instructions, examples, and information to help organizations interpret and apply ISO 22301 and due to its inherently complementary nature it is poised to act as a pivotal implementation guide for best practices in business continuity tailored to the electricity sector's needs.

- **ISO 22317** provides a framework for conducting a business impact analysis (BIA), again with the goal of integrating this process into the BCMS. The standard offers guidelines for determining the impact of disruptions on an organization's processes and activities, helping to prioritize the recovery of operations and services and will be used for the assessment of the impact of disruptions on an entity in the electricity sector and to aid with the prioritization of recovery strategies, ensuring that the most critical areas are addressed first in the BCMS.

- **ISO 22318** focuses on supply chain continuity management as part of the BCMS. This standard provides comprehensive guidance on strategizing, enacting, and refining processes to ensure the continuity of the supply chain and underscores the importance of thorough preparation for, as well as agile response to, any potential disruptions that may occur across the supply chain. Given the increasing prevalence of supply chain disruptions as a significant threat, particularly in the highly interconnected and interdependent electricity sector, an entity operating within this domain cannot afford to overlook the inherent risks associated with its supply chain. Consequently, ISO 22318 will be instrumental in integrating supply chain considerations into the BCMS, ensuring that strategies are in place to manage and mitigate risks effectively and maintain continuity in the face of supply chain challenges.

- **ISO 22330** provides guidelines for people aspects of business continuity as an integral part of creating and managing a BCMS. It offers principles, frameworks, and processes for preparing for, responding to, and recovering from incidents with a focus on the needs and responsibilities towards people involved in or affected by such incidents. Hence, this standard will be used to ensure that the BCMS efficiently addresses the needs, safety, and communication of all personnel, a critical factor in the electricity sector where safety and operational roles are paramount.

- **ISO 27001** is a set of requirements for defining, implementing, operating, and improving an Information Security Management System (ISMS), which proposes the PDCA course of action to ensure the continuous improvement and fortification of the ISMS. In the post-NIS2 era, where cybersecurity threats are prevalent, integrating ISO 27001 into the BCMS, by means of the aforementioned PDCA methodology, will ensure that information security is a core component of business continuity planning, particularly relevant for protecting critical information assets in the electricity sector.

- **ISO 27019** is a sector-specific standard for the energy utility industry. It extends the guidelines of ISO 27002 to the context of process control systems used in the energy utility sector, providing best practices for information security management tailored to the unique requirements, technologies, and risks faced by this sector. Thus, this standard will aid in a more specific approach to the unique information security challenges and technologies in the energy sector, aiding in the provision of more sector-specific countermeasures.

To provide a deeper understanding and further contextualize the application of various ISO standards in the development of a BCMS within the electricity industry, Table 3 aims to offer a comprehensive insight into how this selection of ISO standards can be utilized to formulate a

Plan	**ISO 22301**	identification of requirements for the BCMS
	ISO 22317	identification of critical business functions
	ISO 27019	identification of sector-specific concerns
Do	**ISO 22313**	for detailed BCMS implementation guidelines
	ISO 22317	for BIA guidelines
	ISO 27019	precautions around sector-specific concerns
Check	**ISO 22330**	testing of communication and reporting channels
	ISO 27019	assessment of sector-specific concerns
Act	**ISO 22313**	for process guidelines
	ISO 27019	for sector-specific areas of interest

Table 4: ISO Standards Usage

detailed guideline, tailored specifically for entities operating within the electricity sub-sector of the energy industry, while also incorporating the PDCA methodology [5].

6.4 Electricity Sector BCMS - PLAN Phase

6.4.1 Context Establishment

Understanding the organization and its context is vital for developing any kind of management system, and a BCMS is no exception to the rule. Internal and external factors that have the power to influence an organization, be it positively or negatively, ought to be considered, since they are directly, or even indirectly, relevant to the organization's core objectives. A detailed analysis of applicable factors is shown in Figure 3, which should now also take into account the importance of both technical and organizational resilience strengthening methods; methods that encompass a wide range of tools, including personnel training and development, substantive technical support, procedural planning documents, financial planning for resilience activities, and engagement with external political, economic, social, ecological, legislative, and technological resources [22], [29].

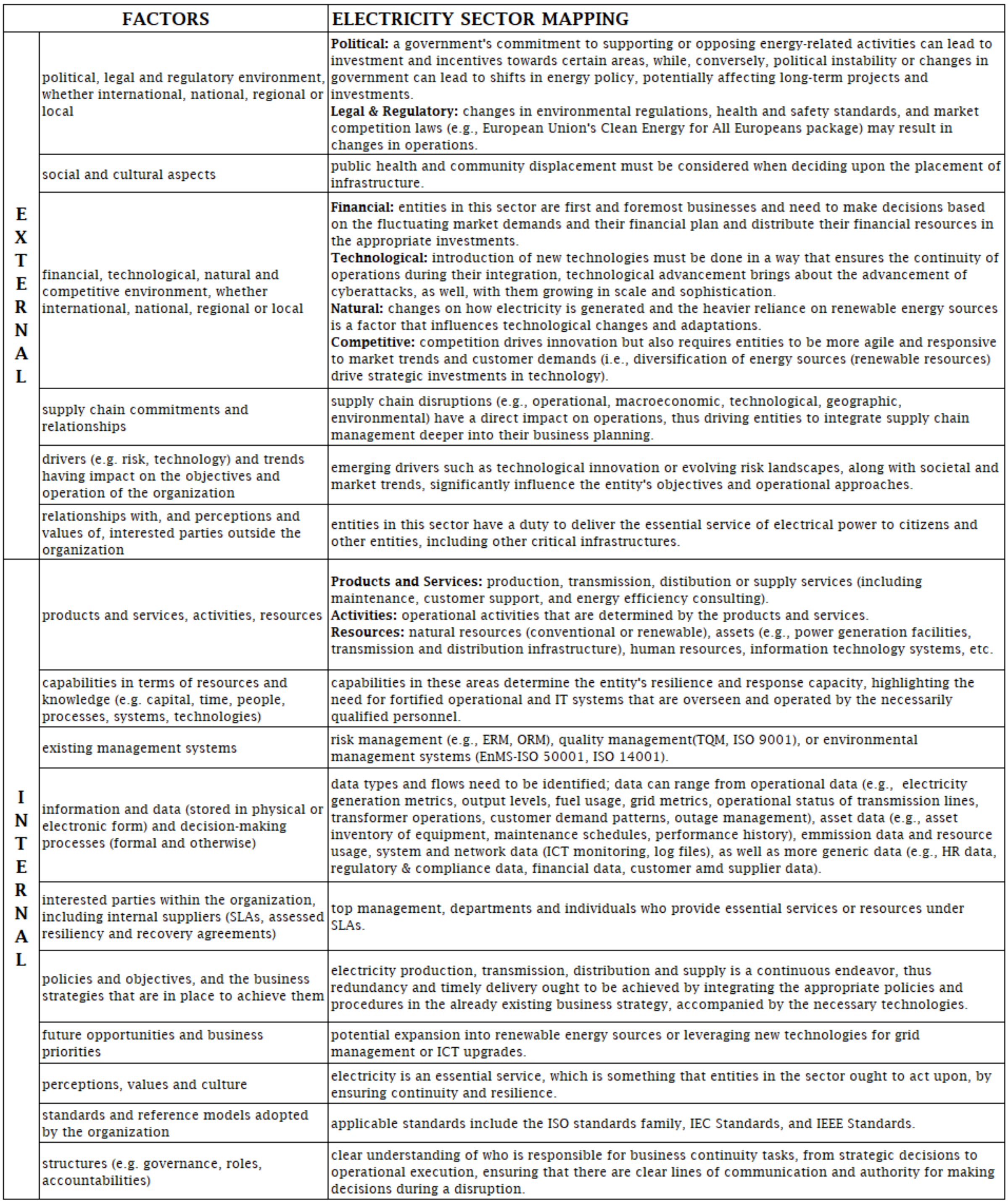
Identify Interested Parties

Interested parties, alternatively called stakeholders, are individuals or organizations that hold the capacity to influence, be influenced by, or consider themselves as being impacted by any decision or activity undertaken by the entity in question. This broad categorization includes but is not limited to, customers, owners, employees, service providers, financial institutions, regulatory bodies, labor unions, partners, and the broader society, which may also encompass competitors or various opposing advocacy groups. It is noteworthy that individuals making decisions, communities and local populations affected by the entity's activities can also be classified as interested parties under this definition.

For an entity in the electricity sector, interested parties can be considered:

- **The management of the electricity facilities**
  Whether we are referring to conventional or renewable resources, electricity facilities encompass a broad range of operations, including power plants that generate electricity, as

[5] [23], [24], [25], [26], [27], [28]



FACTORS		ELECTRICITY SECTOR MAPPING
EXTERNAL	political, legal and regulatory environment, whether international, national, regional or local	**Political:** a government's commitment to supporting or opposing energy-related activities can lead to investment and incentives towards certain areas, while, conversely, political instability or changes in government can lead to shifts in energy policy, potentially affecting long-term projects and investments. **Legal & Regulatory:** changes in environmental regulations, health and safety standards, and market competition laws (e.g., European Union's Clean Energy for All Europeans package) may result in changes in operations.
	social and cultural aspects	public health and community displacement must be considered when deciding upon the placement of infrastructure.
	financial, technological, natural and competitive environment, whether international, national, regional or local	**Financial:** entities in this sector are first and foremost businesses and need to make decisions based on the fluctuating market demands and their financial plan and distribute their financial resources in the appropriate investments. **Technological:** introduction of new technologies must be done in a way that ensures the continuity of operations during their integration, technological advancement brings about the advancement of cyberattacks, as well, with them growing in scale and sophistication. **Natural:** changes on how electricity is generated and the heavier reliance on renewable energy sources is a factor that influences technological changes and adaptations. **Competitive:** competition drives innovation but also requires entities to be more agile and responsive to market trends and customer demands (i.e., diversification of energy sources (renewable resources) drive strategic investments in technology).
	supply chain commitments and relationships	supply chain disruptions (e.g., operational, macroeconomic, technological, geographic, environmental) have a direct impact on operations, thus driving entities to integrate supply chain management deeper into their business planning.
	drivers (e.g. risk, technology) and trends having impact on the objectives and operation of the organization	emerging drivers such as technological innovation or evolving risk landscapes, along with societal and market trends, significantly influence the entity's objectives and operational approaches.
	relationships with, and perceptions and values of, interested parties outside the organization	entities in this sector have a duty to deliver the essential service of electrical power to citizens and other entities, including other critical infrastructures.
INTERNAL	products and services, activities, resources	**Products and Services:** production, transmission, distibution or supply services (including maintenance, customer support, and energy efficiency consulting). **Activities:** operational activities that are determined by the products and services. **Resources:** natural resources (conventional or renewable), assets (e.g., power generation facilities, transmission and distribution infrastructure), human resources, information technology systems, etc.
	capabilities in terms of resources and knowledge (e.g. capital, time, people, processes, systems, technologies)	capabilities in these areas determine the entity's resilience and response capacity, highlighting the need for fortified operational and IT systems that are overseen and operated by the necessarily qualified personnel.
	existing management systems	risk management (e.g., ERM, ORM), quality management(TQM, ISO 9001), or environmental management systems (EnMS-ISO 50001, ISO 14001).
	information and data (stored in physical or electronic form) and decision-making processes (formal and otherwise)	data types and flows need to be identified; data can range from operational data (e.g., electricity generation metrics, output levels, fuel usage, grid metrics, operational status of transmission lines, transformer operations, customer demand patterns, outage management), asset data (e.g., asset inventory of equipment, maintenance schedules, performance history), emmission data and resource usage, system and network data (ICT monitoring, log files), as well as more generic data (e.g., HR data, regulatory & compliance data, financial data, customer amd supplier data).
	interested parties within the organization, including internal suppliers (SLAs, assessed resiliency and recovery agreements)	top management, departments and individuals who provide essential services or resources under SLAs.
	policies and objectives, and the business strategies that are in place to achieve them	electricity production, transmission, distribution and supply is a continuous endeavor, thus redundancy and timely delivery ought to be achieved by integrating the appropriate policies and procedures in the already existing business strategy, accompanied by the necessary technologies.
	future opportunities and business priorities	potential expansion into renewable energy sources or leveraging new technologies for grid management or ICT upgrades.
	perceptions, values and culture	electricity is an essential service, which is something that entities in the sector ought to act upon, by ensuring continuity and resilience.
	standards and reference models adopted by the organization	applicable standards include the ISO standards family, IEC Standards, and IEEE Standards.
	structures (e.g. governance, roles, accountabilities)	clear understanding of who is responsible for business continuity tasks, from strategic decisions to operational execution, ensuring that there are clear lines of communication and authority for making decisions during a disruption.

Figure 3: Mapping context establishment factors to the electricity sector

well as substations involved in the transmission and distribution of electricity [6]. Management at all levels within these facilities (i.e., top management and individuals responsible for the establishment of the BCMS objectives and policies) plays a crucial role for several reasons; firstly, they have an in-depth understanding of the operational intricacies and critical components of their respective facilities, whether these are focused on generation, transmission, or distribution, and whether they involve conventional or renewable energy sources. Their insights are invaluable in identifying potential risks and implementing measures to mitigate these risks, setting a benchmark for operational resilience and ensuring the continuity of electricity supply. Furthermore, the commitment of management to, and their involvement in, the BCMS process are critical for securing the necessary resources, fostering a culture of resilience, and aligning business continuity objectives with the broader goals of the entity (see 5.4.3).

It is important to note that even though the implementation details of the BCMS will certainly differ among the facilities, the overall objectives must be aligned since they all share the common goal of maintaining operations and service provision [31].

- **Professionals responsible for business continuity**
  This group, comprising those who establish and oversee the BCMS, maintain business continuity procedures, and own these procedures, is essential due to the expertise they provide in the development, implementation, and continual improvement of business continuity strategies tailored to the unique demands and operational dynamics of the entity. The group's contributions are pivotal, ensuring that the BCMS remains responsive to evolving challenges and capable of safeguarding the entity's resilience against disruptions.

- **Incident Response Personnel**
  These are individuals authorized to invoke BC plans; it is a group comprised not only of those authorized to initiate the aforementioned plans but also of designated spokespersons responsible for managing communications with internal and external stakeholders, alongside dedicated response teams tasked with executing the tactical aspects of the plan. Their roles are pivotal within the broader spectrum of incident management, as they are the front line in ensuring that the entity's response is both timely and effective and, as a result, sufficient to mitigate the impacts of unforeseen events on operations, ultimately preserving the integrity of the organization's service delivery and operational continuity.

- **Other Staff**
  Including contractors, key staff, support staff, and line managers, this diverse group contributes to the operational resilience of the electricity sector. Their involvement and adherence to BC procedures are vital in maintaining the continuity of operations under adverse conditions, and they will be the ones who have to face the ramifications of machinery malfunction in the cases of field operations.

- **Suppliers**
  Suppliers of critical components and services to the electricity sector are essential for its uninterrupted functioning. Their reliability and commitment to business continuity are integral to the resilience of the electricity supply chain.

[6] the power plants in question can be either thermal (fossil fuel, nuclear or solar thermal power plants), or renewable (hydroelectric facilities, wind turbines, or solar panels)

- **Service Providers**
  External organizations providing essential services, such as IT and communication systems, are critical to the operational capabilities of the electricity sector. Their resilience is directly tied to the sector's ability to manage and recover from incidents.

- **Citizens**
  As the ultimate end-users of electricity, citizens' safety and well-being are of paramount concern, especially during outages or disasters. Their needs and expectations guide the prioritization of critical services and restoration efforts.

- **Government**
  Governments play a regulatory and supportive role, often setting standards for resilience and business continuity. Their involvement is critical in ensuring that the electricity sector adheres to national safety and security standards.

- **Regulators**
  Regulatory bodies enforce compliance with industry-specific standards and guidelines for business continuity and resilience. Their oversight ensures that the electricity sector maintains high standards of operational reliability and safety.

- **Customers**
  Commercial and industrial customers, like citizens, rely on a stable electricity supply for their operations. Their demands and feedback are crucial in shaping business continuity plans and in ensuring the sector's responsiveness to market needs.

- **Emergency Services**
  In the event of a disruption, coordination with emergency services is crucial for ensuring public safety and the protection of critical infrastructure. Their readiness and responsiveness are integral to the sector's incident response strategies.

Legal & Regulatory Requirements

In the process of establishing a BCMS within the electricity sub-sector, entities must rigorously identify and document the legal and regulatory requirements. These requirements, pivotal for ensuring the BCMS's efficacy and compliance, can be categorized as implied, stated, or obligatory. Essential to this endeavour is the entity's ability to maintain an up-to-date repository of these requirements, which encompasses current, pending, and evolving legal and regulatory frameworks relevant to its operations. This includes but is not limited to, areas such as incident response, including emergency management legislation; business continuity, dictating the BCMS's scope or recovery objectives; risk management, outlining the approaches or scopes for risk assessment; and hazards, including operational stipulations for managing dangerous materials. These requirements, including directives and regulations such as the Clean Energy for All Europeans Package, Electricity Market Directive, Renewable Energy Directive, and national transpositions thereof, dictate the operational, environmental, and safety standards that entities must adhere to.

The significance of these requirements extends beyond procedural adherence; they form the bedrock upon which the BCMS is developed, ensuring the system's alignment with legal mandates and regulatory expectations. This alignment is crucial for mitigating risks, facilitating swift recovery from disruptions, and ultimately, safeguarding the continuity of essential services. Moreover, the dynamic nature of legal and regulatory landscapes necessitates continuous monitoring and updating of this information, coupled with effective communication strategies to disseminate changes to affected employees and other interested parties.

For entities operating across multiple jurisdictions, the complexity deepens as they navigate a mosaic of legal and regulatory environments. It is vital for these entities to demonstrate not only their awareness of relevant legal and regulatory requirements but also their adherence to these mandates across different operational locales. This comprehensive approach ensures that the BCMS is not only robust and resilient but also adaptable to the diverse legal landscapes within which the entity operates, thereby reinforcing its commitment to operational integrity, public safety, and the uninterrupted delivery of electricity.

Scope Determination & Exceptions

The outputs of the previous steps will be taken into consideration when determining the scope of the BCMS; namely, any issues found in the context establishment ought to be addressed, as well as all the interests of the stakeholders. First, we need to identify the boundaries and applicability of the BCMS [10], [36].

- **Services & Activities**

  The first step is to examine the entity's services and activities across the various operational levels — production, transmission, distribution, and supply. This analytical approach ensures that the BCMS is comprehensively tailored to address the unique challenges and operational intricacies of each level, thereby enhancing resilience and continuity capabilities. Below is a high-level overview[7] (Figure 4 in the Annex provides indicative operational and organizational processes that need to be identified):

  - **Production Level**

    As stated previously, the production level encompasses entities involved in the generation of electricity from various energy sources, including conventional and renewable, and thus the service provided at this level is that of the **electricity generation**. The activities associated with this include fuel handling, power generation, cooling and condensation, energy conversion and transmission, and waste management and emission control.

  - **Transmission Level**

    The transmission level involves facilities responsible for the high-voltage **transportation** of electricity **from production facilities to distribution networks** across extensive geographical areas. This includes activities such as monitoring incoming power, voltage transformation (step-up), transmission over high-voltage lines and monitoring of the electricity flow.

  - **Distribution Level**

    Distribution facilities are the ones which enable the **delivery** of electricity **from the**

[7] Details regarding the maintenance of equipment, safety checks, and assessments of operational efficiency have not been explicitly stated. This omission is predicated on the assumption that such activities are universally inherent and meticulously executed across all operational levels, thus forming an integral component of standard operational procedures.

transmission system to end-users, including residential, commercial, and industrial customers, at lower voltages. This includes activities such as voltage transformation (step-down), and the distribution of electricity in local distribution lines.

  - **Supply Level**
    Entities at the supply level focus on the **sale and purchase** of electricity to and from the grid, acting as intermediaries between generators and end-users. Something to bear in mind at this level is the existence, or not, of smart grid technologies, since this will change the landscape both in a literal and a figurative sense - by changing the technologies used and the attack surface, respectively.

- **Locations & Resources**
  Analyzing the services and activities across the different levels of the electricity sector requires a thorough understanding of the associated locations, resources, and assets critical to each level's operation. These elements are foundational to the sector's ability to deliver reliable and efficient electricity services.

  - **Production Level**
    Location: Power plants are the primary locations at the production level. These facilities can vary widely in type, including coal-fired, natural gas, nuclear, hydroelectric, wind farms, and solar photovoltaic parks, reflecting the diverse sources of energy generation.
    Resources: The resources at this level are the natural, conventional, or renewable resources utilized for electricity generation. This includes coal, natural gas, uranium, water flow, wind, and sunlight. The choice of resource depends on the type of power plant and its geographical location, which is often chosen based on the proximity to these resources.
    Assets: At the production level, assets include the operational and technological equipment essential for generating electricity. This encompasses turbines, generators, reactors (for nuclear plants), solar panels, wind turbines, and associated control and monitoring systems. These assets are critical for converting natural or conventional resources into electrical energy.
  - **Transmission Level**
    Location: Transmission substations are key locations at this level. These facilities house the equipment necessary to raise or lower the voltage of electricity coming from production facilities for transmission over long distances.
    Resources: The resource at this level is the generator's voltage, which is transformed to high-voltage levels suitable for efficient long-distance transmission. The high voltage reduces energy loss over transmission lines, making it a critical resource for the transmission process.
    Assets: The operational and technological assets here include the transformers that step up the voltage for transmission, transmission lines, towers, and the control systems that monitor and manage the flow of electricity across the grid to ensure stability and reliability.
  - **Distribution Level**
    Location: Power substations, where transformers step down transmission voltages to

distribution voltages, and the distribution grid that delivers electricity to end-users, are the primary locations. These substations are strategically located to serve residential, commercial, and industrial areas.
    Resources: The electricity received from the transmission grid serves as the resource at this level. The step-down transformers reduce the voltage to levels safe for use by consumers, making it available for local distribution.
    Assets: Assets at the distribution level include the step-down transformers, distribution lines, poles, and metering equipment. Additionally, operational technologies for monitoring, controlling, and managing the distribution of electricity to ensure reliability and meet demand are also considered critical assets.

  - **Supply Level**
    Location: The supply level does not have a specific physical location akin to power plants or substations. Instead, it operates through corporate offices and virtual platforms where electricity trading, customer interaction, and energy management services are conducted.
    Resources: The stepped-down voltages received from the distribution grid constitute the resources for the supply level. This electricity is ready for consumption and is traded or sold to end-users, including households, businesses, and industrial facilities.
    Assets: At the supply level, assets primarily include the systems and platforms for energy trading, billing, and customer management. Technological assets like smart meters, customer interface platforms, data analytics systems, and communication networks are essential for delivering supply-level services effectively.

  SCADA systems [8] are also an integral part of the facilities in question, providing monitoring and control capabilities of dispersed assets across vast geographical expanses.

- **Suppliers & Dependencies**
  In the complex ecosystem of the electricity sector, understanding the landscape of suppliers and dependencies across various operational levels is crucial for establishing a robust BCMS. This multifaceted network, spanning from production to supply, encompasses a wide array of interactions with both physical and digital assets, each with its own set of critical suppliers and inherent dependencies. These relationships are pivotal not only for day-to-day operations but also for ensuring resilience in the face of disruptions. The following analysis delves into the specific suppliers and dependencies characteristic of the production, transmission, distribution, and supply levels, as well as the overarching significance of operational and technological assets within the sector. This insight lays the groundwork for identifying potential vulnerabilities and formulating strategic responses to safeguard continuity and reliability in electricity delivery.

  - **Production Level**
    At the production level, the electricity sector heavily depends on a diverse range of suppliers for natural, conventional, or renewable resources essential for power generation. This level's suppliers include those providing fossil fuels, nuclear material, and renewable resource technologies such as solar panels and wind turbines. A critical

[8] A detailed analysis of how SCADA systems operate and the reasons why they are important for entities in the electricity sector can be found in the Annex.

dependency is on the global supply chain for the procurement of these resources and components, making the production level susceptible to disruptions like geopolitical tensions, trade policies, and natural disasters. Additionally, the sector relies on equipment manufacturers for the operational technology required in power plants, underscoring a dependency on specialized suppliers for maintaining continuous and efficient production capabilities.

- **Transmission Level**
  The transmission level depends on suppliers for high-voltage equipment, including transformers and transmission lines, which are vital for electricity transport from power plants to distribution networks. The geographical concentration of component manufacturing introduces a significant dependency on a limited number of suppliers, elevating the risk of supply chain disruptions. Additionally, there's a reliance on technology providers for control systems that manage the power flow across the grid, highlighting a dependency on digital infrastructure suppliers. The transmission level's ability to maintain grid stability and reliability is contingent upon the seamless integration of physical and digital supply chains.
- **Distribution Level**
  Suppliers at the distribution level include manufacturers of transformers, cables, and other distribution infrastructure necessary for stepping down voltage and delivering electricity to end-users. This level exhibits a dependency on a robust logistical network to ensure timely delivery and maintenance of infrastructure, particularly in response to demand spikes or infrastructure damage from environmental events. Additionally, there's an increasing dependence on technology suppliers for smart grid components, such as advanced metering infrastructure, which facilitate more efficient distribution operations and customer interactions. This digital transformation introduces new dependencies on cybersecurity solutions to protect the grid from cyber threats.
- **Supply Level**
  Entities at the supply level depend on a broad spectrum of suppliers, ranging from wholesale electricity markets for the procurement of electricity to technology vendors for billing and customer relationship management systems. There's a critical dependency on the distribution level's infrastructure to ensure that the procured electricity reaches the consumer efficiently and reliably. Moreover, as the sector moves towards more dynamic pricing models and demand response initiatives, there's an increased reliance on data analytics and digital platform providers. This level must navigate dependencies on regulatory compliance services and market analysis experts to adapt to changing market conditions and regulatory landscapes.

Across all levels, the electricity sector's operational continuity heavily depends on the availability and reliability of both physical and technological assets. These assets range from generation equipment and transmission infrastructure to distribution networks and customer interface systems. There's a pervasive dependency on suppliers for the maintenance, repair, and upgrade of these assets, making supply chain resilience critical. The integration of digital technologies introduces dependencies on software vendors and cybersecurity solutions, emphasizing the need for strategic partnerships with technology providers. Ensuring the security, sustainability, and resilience of these assets amidst evolving threats and technological advancements remains a paramount concern for the sector.

- **Exclusions to Scope**
  In the electricity sector, exclusions to the BCMS scope may encompass certain ancillary services or operational facets deemed non-critical to the core mission of delivering uninterrupted electricity to customers. For instance, non-essential administrative functions, certain R&D activities, or secondary facilities not directly involved in the generation, transmission, distribution, or supply of electricity might be considered for exclusion. However, it is imperative that such exclusions are carefully documented with clear justifications, ensuring they do not compromise the organization's capability to adhere to business continuity requirements identified through the business impact analysis (BIA)[9]. Furthermore, in the context of integrating the BCMS into existing management systems, it must be verified that all essential elements of the BCMS are comprehensively included, without overlooking critical dependencies and supply chains necessary for the delivery of in-scope products and services. This approach ensures the resilience of the electricity sector's operations, safeguarding against potential disruptions while maintaining a clear focus on essential services and activities.

6.4.2 Leadership

Both top management and other managerial roles are integral to demonstrating leadership and commitment, ensuring the BCMS is deeply embedded within the organizational culture and operational practices. For the top management, it starts with the clear assignment of managerial roles, specifically appointing individuals with the requisite authority and competencies to oversee the BCMS, ensuring its effectiveness and alignment with the organization's goals. Additionally, top management is responsible for fostering an environment of continual improvement, ensuring BCMS objectives are met, and providing support to other management levels to enable their leadership roles. Indicatively, the top management ought to strive for the following:

- **Recruitment and Development of Qualified Personnel:** Top management should prioritize the recruitment and ongoing development of highly skilled individuals tasked with overseeing the BCMS and relative operations. This team should include professionals with expertise in operational technologies utilized within the sector, such as SCADA systems, as well as cybersecurity experts who can address the unique challenges of protecting critical infrastructure. Ensuring that these individuals are well-versed in the latest industry standards and best practices is crucial for the effective development, implementation, and management of the BCMS policy and procedures.

- **Provision of Necessary Resources and Investments:** Committing to and securing the necessary resources and financial investments are essential actions that top management must undertake. This includes allocating funds for the acquisition of state-of-the-art technology, supporting infrastructure enhancements, and investing in employee training programs. Adequate resourcing also encompasses ensuring sufficient staffing levels to

[9] The business continuity requirements can be derived from the BIA once the PDCA cycle has been already completed once. In the first implementation of the BCMS, requirements can be identified sufficiently through the previous steps of the context establishment phase, and then be enriched as the PDCA cycle continues.

manage and respond to incidents, emphasizing the importance of resilience and continuity across all operations.

- **Fostering a Culture of Continuous Improvement:** Top management must champion a culture of continuous improvement within the organization. This involves encouraging open communication about potential risks and vulnerabilities, learning from incidents and near-misses, and regularly reviewing and updating the BCMS to adapt to changing threats and operational demands. By promoting an environment where employees at all levels are motivated to contribute to the BCMS's effectiveness, top management can drive the ongoing enhancement of business continuity practices.

- **Commitment to Compliance and Best Practices:** Ensuring adherence to legal, regulatory, and industry-specific standards is critical. Top management should demonstrate a commitment to compliance with frameworks such as ISO 22301, as well as local and international regulations governing the electricity sector. This includes regular audits, assessments, and adjustments to the BCMS to align with best practices and legal requirements.

- **Engagement and Communication with Stakeholders:** Actively engaging with internal and external stakeholders, including employees, customers, suppliers, and regulatory bodies, is essential. Top management should lead by example in communicating the importance of business continuity and the BCMS's role in ensuring the organization's resilience. This includes transparently sharing information about BCMS initiatives and encouraging feedback and collaboration from all stakeholders.

Managers at various levels are tasked with integrating the BCMS into business processes, setting objectives that support the entity's strategic direction, and ensuring awareness and compliance with legal and regulatory requirements. Their leadership is also demonstrated through the establishment of clear roles, responsibilities, and competencies within the BCMS, active participation in exercise programs, conducting internal audits, and leading effective management reviews of the BCMS. These actions are vital for achieving the intended outcomes of the BCMS and directing its continual improvement. Table 5 outlines indicative roles and responsibilities [33]. Beyond formal responsibilities, the management's commitment is further evidenced by operational involvement, such as participation in steering groups and using a staircase or capability maturity model to illustrate progress in business continuity capabilities [20], making business continuity a standard agenda item at management meetings. This approach ensures a gradual improvement in the entity's ability to handle crises, emphasizing the necessity of continuous engagement and maintenance to prevent regression. This ongoing engagement ensures that business continuity considerations remain a focal point of decision-making processes, reflecting a deep-rooted culture of resilience across the organization.

The creation of a business continuity policy is a critical step in establishing the BCMS since it serves as a high-level statement reflecting the entity's commitment to maintaining electricity supply and managing disruptions effectively. It must articulate its dedication to objectives, obligations, and continual improvement, incorporating legal and regulatory compliance as fundamental components. Given the sector's CI status, where mishaps or successful attacks could not only result in service disruption, but also endanger human life, the policy should outline the scope and boundaries of BC efforts and clearly define the authorities, responsibilities, and funding commitments related to BC management. This document should, also, reference applicable standards, guidelines, and policies, ensuring alignment with industry best practices and regulatory requirements. Moreover, the policy should emphasize the importance of periodic reviews and updates in response to significant changes in internal or external factors, such as new legislation or shifts in operational environments, ensuring its relevance and effectiveness over time, which will inevitably occur once the PDCA cycle will be completed and re-initiated and the entity will have to revise its context.

This approach not only ensures operational resilience but also reinforces the sector's commitment to safeguarding the continuous delivery of electricity to consumers and businesses alike.

6.4.3 Planning

After laying the groundwork described in the previous sections, now is the time to devise an action plan to manage issues and risks derived from the context establishment, as well as establish clear, actionable business continuity objectives.

Risk Identification and Mitigation Planning

Firstly, the entity should systematically identify risks that have been highlighted through the context establishment process. This involves understanding both external and internal factors that could potentially disrupt operations, including but not limited to, supply chain vulnerabilities, technological failures, natural disasters, and cybersecurity threats. Upon identifying these risks, the organization must then plan on how to address them. This could involve implementing technical solutions such as upgrading infrastructure or software to withstand cyber-attacks or organizational measures like revising supply chain strategies to reduce dependency on single sources.

Establishing and Determining Business Continuity Objectives

Concurrently, the entity must establish its business continuity objectives, that align with the overall organizational goals, ensuring they contribute to the overarching mission while addressing specific areas for improvement identified in the BCMS. Responsibilities for achieving these objectives must be clearly assigned, with realistic targets set for completion, and mechanisms for monitoring progress and evaluating results firmly in place. For instance, an objective could be as specific as "Reducing the recovery time objective (RTO) for critical electricity distribution activities by 15% within the next fiscal year, overseen by the Operations Director." Communicating these plans and objectives throughout the organization is crucial for ensuring alignment and commitment across all levels. This also involves regular monitoring, documentation of progress, and incorporating feedback mechanisms for continuous improvement.

It is important to acknowledge that in the initial establishment of the BCMS, this step's outputs might not be extensively detailed. It is feasible to delineate general objectives concerning continuity and resilience; however, the articulation of concrete milestones and the specification of organizational or technological measures may necessitate the completion of one full PDCA

Roles	Responsibilities
BCMS Manager	oversees the development, implementation, and maintenance of the BCMS coordinates business impact analysis, audits and risk assessments and reports on BCMS performance to top management liaises with all departments to ensure BCMS integration into daily operations leads incident response and recovery efforts
Business Owner	makes key decisions about how the entity handles incidents
Technical Services Manager	manages disruptions to technical services, such as IT infrastructure and applications interacts with third-party business continuity service providers
Operations Manager	integrates BCMS processes into operational procedures ensures operational readiness and resilience manages the operational response during disruptions coordinates with BCMS Manager for incident response planning & execution
Communications Manager	develops & executes communication plans for internal and external stakeholders during disruptions manages public relations & media inquiries related to business continuity ensures clear and consistent communication during incidents
Estate Manager	ensures the physical security and resilience of facilities manages disruptions relating to buildings, offices, and the surrounding environment initiates continuity arrangements and interacts with third-party business continuity service provider
Supply Chain Manager	assesses and manages supply chain risks affecting business continuity develops and maintains relationships with key suppliers to ensure supply chain resilience coordinates alternative supply strategies during disruptions
Business Operations & Customer Services Manager	manages disruptions relating to buildings, offices, and the surrounding environment initiates continuity arrangements and interacts with third-party business continuity service provider
BC Team	technical, estate, or customer services teams that execute the BC plans
Legal & Compliance Officer	ensures the BCMS complies with legal, regulatory, and industry standards advises on legal considerations in BC planning and recovery efforts manages regulatory reporting and documentation requirements

Table 5: BCMS Roles & Responsibilities

cycle, allowing the entity to identify inefficiencies and areas needing improvement, first, and then strive to make the necessary improvements, thereby refining the BCMS's efficacy and responsiveness to identified risks and challenges.

6.4.4 Support

Resources

The successful implementation and sustenance of the BCMS hinge critically on the determination and provision of the necessary resources, which are fundamental not only to achieving the established BC policy and objectives but also to adapting to the evolving requirements of the entity. Effective communication, both internally and externally, about BCMS matters, and the assurance of the BCMS's ongoing operation and continual improvement, are paramount for the resources to be available in a timely and efficient manner to respond promptly to business continuity needs. Identifying BCMS resources encompasses a broad spectrum, including the allocation of personnel, facilities and infrastructure; all crucial for the industry reliant on physical assets for the generation, transmission, and distribution of electricity. Information and Communications Technology (ICT) systems are indispensable for supporting program management and ensuring robust communication channels.

Personnel - Training - Awareness

Managing the competence of personnel involved in BCMS roles is crucial for ensuring operational resilience and safety. The entity must establish a systematic approach for competence management, encompassing the identification of necessary competencies for all BCMS roles and responsibilities. This includes the awareness, knowledge, understanding, skills, and experience essential to effectively fulfil these roles. Additionally, the organization should ensure the recruitment or contracting of individuals who already demonstrate the required competencies. Target groups within the organization should receive specialized training, with activities meticulously documented and monitored to evaluate the effectiveness and conformity with BCMS training requirements. This evaluation should guide the continuous improvement of the development program, ensuring it remains aligned with evolving business continuity needs.

For contractors and external parties working on behalf of the organization, it is imperative to require demonstrations of competence in BCMS-related roles, ensuring they meet the standards expected for effective business continuity management. This holistic approach to competence management in the electricity sector ensures that the organization is not only equipped with the necessary skills and knowledge for business continuity but also fosters a culture of continuous improvement and resilience.

The organization should implement an awareness program that includes various activities aimed at ingraining business continuity awareness across all levels. These activities could range from consultations and discussions featured in newsletters and orientation programs to the inclusion of business continuity topics in staff and management meetings, and regular communications with suppliers to ensure they comprehend and can meet the organization's continuity requirements. Moreover, the organization should demonstrate awareness of business continuity management trends and actively participate in industry-related activities to stay abreast of best practices and innovations.

Embedding business continuity management within the organization's culture is supported by involving all personnel, fostering distributed leadership, assigning clear responsibilities, utilizing performance indicators, integrating continuity into regular management practices, raising awareness, providing skills training, and regularly exercising business continuity plans. Such a comprehensive approach ensures that business continuity considerations are integral to decisions at all levels, thereby fostering an environment that prioritizes continuous improvement and resilience against disruptions.

Communication

Establishing effective communication strategies is a pivotal aspect of the Business Continuity Management System (BCMS), essential for addressing the needs and expectations of all interested parties, including employees, customers, suppliers, regulators, and the wider community. Effective communication not only facilitates transparency and trust but also ensures coordinated responses during disruptions, enhancing the organization's resilience and operational continuity.

The entity must meticulously define the scope of BCMS-related communications, taking into account legal, and regulatory obligations, and the specific context of the electricity sector. This includes:

- Content: Identifying the information to be communicated, which may vary depending on the situation, such as updates during an incident, changes to business continuity plans, or responses to regulatory changes.
- Timing: Establishing when communication should occur, including setting thresholds for initiating communication during disruptions and determining the frequency of updates to ensure timely and relevant information dissemination.
- Audience: Understanding the diverse communication needs of all interested parties and prioritizing communication efforts accordingly. This involves mapping out stakeholders and determining the specific circumstances under which each requires communication.
- Methods: Predefining the channels, tools, and methods for delivering messages, including digital platforms, social media, press releases, and direct communications. Alternative means should be identified to ensure redundancy.
- Execution of Communication: Assigning spokespersons and contact points within the organization who are authorized and trained to communicate on behalf of the organization during various situations.

Incorporating information about the BCMS and business continuity arrangements in communications with suppliers and customers (e.g., with briefings) can bolster awareness and preparedness. Effective external communication is crucial, both as a component of the overall awareness program and in the immediate response to incidents, ensuring stakeholders are informed, engaged, and aware of the organization's preparedness and response strategies.

Documentation

Managing documented information is a cornerstone of establishing and maintaining an effective BCMS. This encompasses a wide range of documentation, from understanding the organizational context and legal requirements to detailing the BCMS scope, policies, objectives, and specific business continuity plans and procedures. Critical to this documentation are the results of business impact analyses, risk assessments, and the selection of business continuity strategies, which inform the development of comprehensive and actionable continuity plans tailored to the sector's unique challenges, such as grid stability, supply chain vulnerabilities, and cybersecurity threats.

Creating and Updating Documented Information

The creation and updating of documented information should adhere to stringent criteria to ensure clarity, reliability, and relevance. Each document must be identifiable through attributes like name, reference number, and version, with specified formats and media for storage ensuring consistency and accessibility. The appropriateness of the format and media is crucial for the document's adequacy in supporting BCMS objectives, taking into account the organization's size, the complexity of its operations, and the competence of its personnel.

Control of Documented Information

Controlling access to documented information involves establishing levels of permission to prevent unauthorized modifications or deletions and to protect sensitive data. This is especially pertinent in the electricity sector, where documents may contain sensitive operational data or detailed recovery procedures that, if compromised, could impact the sector's security and resilience. Documented procedures must define controls for document distribution, access, approval, review, and updates, ensuring that all documents are current, legible, and accessible only to authorized personnel. The protection of these documents against tampering, loss, or damage is vital, along with compliance with legal regulations regarding document retention.

In the electricity sector, where the operational environment is complex and highly regulated, the documentation process must be rigorous yet flexible enough to adapt to changing conditions and regulatory requirements. This includes maintaining evidence of inspections, maintenance, calibration activities, post-incident reports, and communications with suppliers and contractors, ensuring that all aspects of the BCMS are documented, controlled, and continually improved. Through diligent management of documented information, entities in the electricity sector can enhance their BCMS's effectiveness, ensuring readiness and resilience in the face of disruptions while safeguarding critical infrastructure and the communities they serve.

6.5 Electricity Sector BCMS - DO Phase

After concluding the Plan phase, the entity must start the implementation of the BCMS [10] considering the following:

1. BC Policy
   which reflects the management's commitment to business continuity and outlines the objectives, guiding principles, and strategic direction for the BCMS, with clearly defined roles and responsibilities.

2. BCMS Scope
   a clearly defined scope which encompasses critical areas and functions of the entity that are essential for its operational continuity.

[10] or the implementation of corrective actions if the PDCA cycle has already been completed once

3. Available Resources
   resources can include personnel, technology, information, financial resources, and other assets necessary for establishing and maintaining BC procedures that will ensure the support of the BCMS to meet the objectives and requirements of the BC policy.

4. Action Plan
   a plan for the implementation process, with tasks, timelines, and milestones for setting up (or enhancing) the BCMS.

Resource Allocation & Implementation of Controls and Procedures

Having identified the available resources, they need to be allocated accordingly to facilitate the execution of the BC policy and the procedures that will be described in this section. While doing so, the creation, update, and control of documented information needs to be ensured, whether that be new policies, plans, and procedures, or the correction of already existing ones.

Business Impact Analysis & Risk Assessment

Business continuity priorities and requirements are stated and justified as a result of the BIA process, which examines the effects of an interruption on the entity that conducts it; a crucial step for understanding the potential impact of disruptions to operations and establishing recovery priorities. After identifying critical business functions and their potential impacts, a risk assessment is conducted to identify the threats and vulnerabilities that could lead to such disruptions. This step assesses the likelihood of various risks materializing and their potential impact on the organization's operations. While the RA can be initiated after the BIA, in practice, it's often a concurrent process where insights from the BIA inform the RA, particularly in identifying which risks to focus on. The BIA provides crucial data for the RA by highlighting which business functions are most critical and what the potential impacts of their disruption might be. This information helps prioritize risk management efforts towards the most significant processes and risks, respectively. Although the BIA typically precedes or informs the RA, there's a cyclical or iterative relationship between the two. Insights from the RA can lead to revisiting and updating the BIA, especially as new risks are identified or as the business environment changes.

The BIA steps are the following:

1. Plan BIA
   Given the outputs of the Pan phase, mentioned above, a team is being assembled to conduct the assessment. Since the resources, the roles and responsibilities, the scope and the management's commitment are confirmed, this step primarily involves grouping and scheduling activities, defining templates or tools to be used and communicating with activity owners.

2. Determine & Measure Impacts
   Considering the interested parties and the internal and external factors identified in the Plan phase, the entity can decide upon the types of impacts resulting from the disruption to the delivery of services. More specifically, an entity in the electricity sector will potentially face the following impacts:

   - **Client & Societal Backlash:** should electricity provision cease operations in the face of a disruption, the consumers will not have electrical power to conduct their daily activities or their duties. Even though this could be mitigated from the side of the consumers (e.g., with electricity generators or UPSs) should the unavailability last for extended periods of time, the consequences will be harder to manage.

- **Staff Endangerment:** disruptions in any of the operational levels could be the result of equipment failure, a natural disaster or a cyberattack that rendered technologies, processes or equipment unavailable. Whichever the cause, should such negative consequences come to fruition, the physical integrity of the entity's employees could be at stake, ranging from bodily harm to the endangerment of human life.
- **Asset Damage:** a result of aging infrastructure, a natural disaster or a cyberattack, damaged equipment and facilities may cause significant hurdles. Their prompt restoration needs to be given priority over other activities in order to resume operations as swiftly as possible (e.g., damaged assets in the production level shall have a cascading effect on the rest of the levels).
- **Loss of Shareholder Trust:** given the magnitude of the disruption, shareholders may decide to withhold future investment endeavours.

Regarding types and severity, the above can be categorized as shown in Table 6 and further details regarding types and severity can be found in the Annex (Figures 5 and 6). Especially for entities in the electricity sector, time frames must be defined for impact quantification purposes (e.g. at 1 hour, at 6 hours, at 24 hours, etc.). These should be accompanied by the following time frames:

- Maximum Period of Tolerable Disruption (MTPD): the maximum amount of time that a process or function can be disrupted without causing irreparable damage to the organization. It essentially defines the threshold of tolerance for disruption beyond which the entity's viability may be at risk.
- Recovery Time Objective (RTO): a specific duration within which a business process must be restored after a disruption to avoid unacceptable consequences associated with a break in business continuity. The RTO is a target time set for the recovery of IT systems, applications, and functions after an outage and is a fundamental part of disaster recovery and business continuity planning. The RTO is often established based on the criticality of the business process and the MTPD, ensuring that recovery efforts align with the organization's tolerance for downtime, and it cannot be longer than the MTPD.

Furthermore, due to the criticality of the activities and services, when conducting a BIA the analysis ought to be predicated on the idea that the disruption happens at the worst time, and the worst scenario ought to be recorded.

3. **Services Prioritization:** now the top management shall decide upon the services that will receive higher priority over others. To make decisions, top management ought to consider key factors, which include, but are not limited to, the defined missions, objectives, scope and dependencies, legal, regulatory, and contractual requirements, and, if applicable, lessons learned from past disruptions and PDCA cycle exercises. For instance, if there are disruptions which ultimately limit the electricity flow, a choice may be made to prioritize electricity provision to critical infrastructure facilities, over a residential area.

The outcomes should be a list of prioritized services and their continuity requirements which will be used in the next step.

4. **Activity Prioritization:** given the scope, impacts and priorities, activities to be conducted in the face of disruptions must be outlined, each with its RTO. Given the landscape/environment of each process or service, a list of activities which aim for operational continuity and consequence mitigation needs to be assigned to each process and their prioritization will be decided based on their RTO. Each of the activities shall have the following factors defined: interdependencies and relationships between the respective services and other activities, identified impacts, a corresponding MTPD and RTO, and a minimum acceptable results capacity.

5. **Resources & Dependencies:** following the identification of prioritized activities it is crucial to gain an understanding of the resource requirements essential for their recovery or maintenance. This process involves cataloguing resources and dependencies that are critical to operational continuity. For each identified resource, the entity must collect detailed information on the quantity required—considering potential reductions or increases in capacity needs over time, the specific time frames for resource availability, and the unique characteristics of each resource type, such as staff qualifications or IT equipment specifications. Additionally, understanding the maximum tolerable data loss for informational resources and identifying dependencies among resources is imperative. This analysis also extends to recognizing legal or regulatory requirements affecting resource utilization.

6. **Results Analysis:** upon completing the BIA, the next step involves the final analysis or consolidation of analyses, which is pivotal for synthesizing the validated and approved information gathered across all levels of the BIA, with the objective of deriving concrete conclusions that establish clear business continuity priorities and requirements. This process may uncover recovery objectives that are incompatible or unrealistic, necessitating a collaborative review with the activity owners to address and rectify these discrepancies. A notable consideration during this phase is the potential need to adjust the RTOs of predecessor activities, making the overall strategy more achievable.

7. **BIA Approval:** securing the top management's approval for the BIA results is essential in the business continuity planning process; the BIA leader must present the prioritization of products, services, processes, activities, and resources to management for review, amendment, and approval, ensuring alignment between business continuity planning and the organization's strategic goals.

8. **Review BIA:** this review encompasses both the methodology used for the BIA (e.g., re-evaluating the impact types, time frames, data collection methods, or participants involved in the process) and the results it yields (e.g., due to organizational or regulatory changes, operational upgrades, etc.), ensuring they remain relevant and reflective of the organization's current operating context.

For the risk assessment, the entity shall conduct a detailed examination of the organization's vulnerabilities and the external and internal threats it faces, assessing the likelihood of occurrence and the potential impact on the entity's critical functions. Drawing heavily on data and insights from the Business Impact Analysis (BIA), the RA focuses on pinpointing which

Impact	**Type**	**Level of Impact**
Client & Societal Backlash	Reputational / Business Objectives	Depends on the duration of the disruption and the number of customers affected
Staff Endangerment	Health & Safety	Depends on the outcome, but considering the nature of the impact, it should be classified as one of the most severe
Asset Damage	Operational	Depends on the number/importance of assets (e.g. a large number of damaged assets may render redundancy not possible, or a highly critical asset must be replaced instantly)
Loss of Shareholder Trust	Reputational	Depends on the extent of the gathered attention

Table 6: Impacts matrix for entities in the electricity sector

risks merit the most attention based on their probability and potential to affect vital business processes. The threats identified in section 4.4 can be used as a starting point.

Business Continuity Strategies & Solutions

Based on the outcomes of the BIA and risk assessment, the entity shall identify and select appropriate business continuity strategies and solutions to mitigate the impact of identified risks, ensuring the selected strategies and solutions address the prioritized activities and resources identified in the BIA [4].

A designated Incident Response Team (IRT), a specialized group tasked with implementing the organization's incident response plan when a disruption occurs, will be the one to drive the recovery efforts forward. It is typically composed of members from various departments, including IT, security, legal, public relations, and human resources, reflecting the multifaceted approach needed for effective incident management. Members are selected based on their skills, knowledge, and abilities relevant to incident response, including technical expertise, communication skills, and decision-making capabilities.

Exercise & Evaluate

Exercises, including tests, are critical activities designed to assess the entity's capability to effectively respond, recover, and maintain business functions in the face of disruptive events. By conducting these exercises and documenting the outcomes, the entity can gauge the performance of its BC strategies in real scenarios, providing a basis for refining and enhancing its BCMS.

The evaluation focuses on a comprehensive review of key BCMS components, including the Business Impact Analysis (BIA), risk assessments, business continuity strategies, solutions, and related plans and procedures. The primary goal of this evaluation is to verify the accuracy, relevance, and effectiveness of these components, ensuring they are meticulously documented and align with the entity's current needs and the dynamic nature of its operational environment, whichj is crucial for confirming that the BCMS remains pertinent and functional amidst organizational or environmental changes. It also examines the practicality and operational viability of the strategies and plans, it assesses whether these plans can be effectively put into action and if they comprehensively cover all critical operational areas as intended. This process is geared towards confirming operational readiness and the tangible applicability of the planned BC measures, underscoring the importance of not only having a well-documented BCMS but also ensuring that it is operationally sound and ready to be deployed when necessary.

6.6 Electricity Sector BCMS - CHECK Phase

This is the performance evaluation phase of the entire BCMS. his phase is detailed through Monitoring and Measurement, Internal Audit, and Management Review components.

Monitoring and Measurement: this process extends beyond the confines of documentation review, delving into the broader operational performance of the BCMS. It involves continuous monitoring and measurement activities designed to collect data on how the BCMS performs in relation to predefined objectives and metrics. The focus here is on assessing the overall functionality of the BCMS, ensuring that it meets its intended goals and operates effectively as a cohesive system.

Internal Audit: the internal audit serves as a comprehensive evaluation of the BCMS, employing a systematic, independent approach to gather and assess audit evidence. This process is aimed at verifying the extent of conformity with audit criteria, encompassing not just a review of the BCMS documentation but also assessing the effectiveness of its implementation and operation. The audit scrutinizes adherence to the BCMS policy, checks compliance with ISO 22313 standards, and evaluates the system's overall performance. Essentially, the internal audit acts as a thorough health check, identifying areas of strength and opportunities for improvement within the BCMS.

Management Review: the management review involves senior management evaluating the BCMS's performance data and audit outcomes, ensuring that the BCMS remains aligned with the strategic direction of the entity, is adequately resourced, and continues to meet legal, regulatory, and business requirements. It facilitates informed decision-making regarding necessary adjustments or enhancements to the BCMS, ensuring its continual improvement and relevance in an ever-changing operational landscape.

6.7 Electricity Sector BCMS - ACT Phase

The focus of this phase is addressing non-conformities and driving continual improvement to ensure the BCMS's effectiveness and efficiency.

Nonconformity & Corrective Actions

The entity is required to identify and manage nonconformities, which include failures to meet requirements, ineffective planning, or weaknesses in the BCMS. This involves establishing procedures for early detection, analysis, and elimination of both actual and potential causes of nonconformities. Corrective actions should be timely, clearly defined, aimed at mitigating consequences, restoring normal operations, and preventing recurrence by addressing root causes, and their scale should match the severity of the nonconformity. Procedures should also be in place to ensure that improvements are pursued even in the absence of explicit nonconformities, encompassing corrections, corrective actions, innovation, and reorganization, with top management ensuring implementation and effectiveness evaluation. Additionally, it is important to retain documented evidence of nonconformities, actions taken to address them, and the outcomes of such corrective actions. Furthermore, this strategic approach to BCM within the electricity sector can significantly contribute to the sector's ability to anticipate, prepare for, respond to, and recover from disruptions, thereby aligning corrective actions with broader strategic objectives and competitive advantage preservation [18].

Continual Improvement

This is an overarching goal that applies across all levels of the BCMS and the entire PDCA cycle, driven by policy, objectives, audit findings, analysis of disruptions, and management reviews. It involves identifying opportunities for improvement and implementing necessary changes to enhance the BCMS's suitability, adequacy, and effectiveness and it can stem from various sources, including organizational context changes, internal structure modifications, production or delivery methods advancements, technological or methodological innovations, and changes in the threat landscape. These opportunities should be systematically evaluated to determine their potential to elevate the entity's BCMS. Recognizing BCM not just as a functional requirement but as a strategic tool that contributes to operational continuity and resilience against threats, and, as such, continual improvement efforts should also focus on enhancing the strategic integration of BCM, ensuring that it is deeply embedded within the electricity sector's operations. This strategic embedding facilitates a more proactive, comprehensive approach to managing business continuity risks and aligns with the sector's objectives of ensuring uninterrupted electricity supply. Ultimately, the epitome of the entity's commitment to continual improvement is the re-initiation of the entire PDCA cycle, now equipped with more knowledge and insights.

7 Conclusion, Contribution & Future Research

Delving extensively into the field of business continuity in the electricity sector, it is apparent that its scope and complexity are the factors that significantly increase the challenges and demands of business continuity endeavours. The intricate web of dependencies, alongside the critical nature of uninterrupted electricity production, transmission, distribution and supply, underscore the necessity for business continuity procedures to be both precise and up-to-date. In this sector, even minor disruptions can ripple through the economy and society, making it imperative for business continuity strategies to meticulously account for a wide array of potential scenarios and responses. This complexity not only makes the planning process more laborious but also elevates the importance of regular updates and revisions to ensure plans remain relevant and effective against evolving threats and vulnerabilities, but also the environment in which the entities operate.

The NIS 2 directive updating its scope to delineate among the entities found in the electricity sector shows that the complexities inherent within it are recognized and in need of a more targeted approach moving forward, especially considering the ever-evolving landscape of cyberattacks. By adopting a BCMS that aligns with the ISO family of standards, as detailed in this thesis, entities across the electricity sector spectrum can find a structured pathway to either establish or enhance their business continuity approach and procedures. The mappings provided herein serve as a tool, offering clear guidance for these entities to tailor their business continuity practices effectively. This ensures not only compliance with international standards but also fortifies their resilience against cyber disruptions, thereby contributing to the overall security and reliability of the energy infrastructure. This thesis aims to facilitate a deeper understanding and practical application of these standards, fostering a culture of continuous improvement and adaptive defence mechanisms within the sector.

Future research endeavours will aim at delving deeper into the nuanced intricacies of the electricity sector, its four operational levels to be more precise. By conducting thorough on-field research, these investigations shall aim to unearth the specific challenges and opportunities inherent within each level, from generation and transmission to distribution and retail, with the objective being to develop a tailored framework for each of these sectors, one that is both comprehensive and adaptable, reflecting the unique operational, regulatory, and cybersecurity landscapes they inhabit. This focused approach will enable a more granular understanding of the sector's needs, facilitating the creation of bespoke strategies that enhance resilience, operational efficiency, and cybersecurity posture. Ultimately, these frameworks will serve as foundational pillars for guiding the electricity sector's continuous evolution, ensuring its capacity to meet current challenges while anticipating future demands.

References

[1] Ahlqvist M. and Es V. (2023) *Cyber-Physical Security and Critical Infrastructure*, International Security Ligue White Paper. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjGkvfb05KFAxWghP0HHYjKBCIQFnoECBIQAQ&url=https%3A%2F%2Fwww.coess.org%2Fdownload.php%3Fdown%3DLi9kb2N1bWVudHMvaXNsLWNvZXNzLWN5YmVycGh5c2ljYWxzZWN1cml0eS13cC5wZGY.&usg=AOvVaw3n6yuedYej33RwQvF15enq&opi=89978449

[2] Alcaraz C. and Zeadally S. (2015) *Critical infrastructure protection: Requirements and challenges for the 21st century*, International Journal of Critical Infrastructure Protection Vol. 8, p. 53-66.

[3] Australian Government - Department of Home Affairs - Cyber and Infrastructure Security Centre (2023) *Critical Infrastructure Annual Risk Review.*

[4] Azadi M., Olsen P., Wang P., Zare H. and Zare M. (2020) *Business Continuity Plan and Risk Assessment Analysis in Case of a Cyber Attack Disaster in Healthcare Organizations*, 17th International Conference on Information Technology–New Generations (ITNG 2020), p. 137-144. https://doi.org/10.1007/978-3-030-43020-7_19.

[5] Ciobanu, C. et al. (2022). *ENISA THREAT LANDSCAPE 2022.* European Union Agency for Cybersecurity (ENISA), 8-12, DOI: 10.2824/764318. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[6] Ciobanu C., Lella I., Magonara E., Malatras A., Naydenov R., Theocharidou M. and Tsekmezoglou E. (2023). *ENISA THREAT LANDSCAPE 2023.* European Union Agency for Cybersecurity (ENISA), DOI: 10.2824/782573. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[7] CISA (2019) *A Guide to Critical Infrastructure Security and Resilience.*

[8] COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection (Brussels, 12.12.2006)

[9] COUNCIL DIRECTIVE 2008/114/EC

[10] Curtis P. and Mehravari N. (2015) *Evaluating and Improving Cybersecurity Capabilities of the Energy Critical Infrastructure*, IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 2015, p. 1-6. DOI: 10.1109/THS.2015.7225323.

[11] *European critical infrastructure Revision of Directive 2008/114/EC*

[12] Desai S., Jose N., Shelke Y., Srivastava S. (2020) *INDUSTRIAL CYBERSECURITY RISKS - OIL AND GAS OPERATIONS*, InfoSys White Paper. Retrieved from https://www.infosys.com/services/cyber-security/documents/oil-gas-operations.pdf?utm_source=infosys_hub&utm_medium=main

[13] Ding J., Karim A., Ning H., Qammar A. and Zhang Z. (2022). *Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions.* Energies, 15(18). Retrieved from https://doi.org/10.3390/en15186799

[14] Douligeris C., Lourenço M., Marinos L., Raghimi O. and Sfakianakis A. (2018). *ENISA Threat Landscape Report 2018*

[15] Dragomir A. (2021) *What's New in the NIS 2 Directive Proposal Compared to the old NIS Directive.*

[16] Ducuing C. (2021) *Understanding the rule of prevalence in the NIS directive: C-ITS as a case study*, Computer Law and Security Review Vol. 40. Retrieved from https://doi.org/10.1016/j.clsr.2020.1055140267-3649/202

[17] Ehsan F., Rasool G., Shahbaz M. (2015) *A systematic literature review on electricity management systems*, Renewable and Sustainable Energy Reviews Vol. 49. Retrieved from http://dx.doi.org/10.1016/j.rser.2015.04.054

[18] Elliott D., Herbane B. and Swartz E. (2004) *Business Continuity Management: time for a strategic role?*, Long Range Planning Vol. 37, p. 435-457. DOI: 10.1016/j.lrp.2004.07.011

[19] Ferguson D. (2023) *The outcome efficacy of the entity risk management requirements of the NIS 2 Directive*, International Cybersecurity Law Review (2023) Vol. 4, p. 371–386. Retrieved from https://doi.org/10.1365/s43439-023-00097-8

[20] Hägerfors A., Lindström J. and Samuelsson S. (2010) *Business continuity planning methodology*, Disaster Prevention and Management: An International Journal, Vol. 19 Iss 2 p. 243 - 255. Retrieved from http://dx.doi.org/10.1108/09653561011038039

[21] Holzleitner M.T.,Reichl J. (2016) *European provisions for cyber security in the smart grid – an overview of the NIS-directive*, Elektrotechnik & Informationstechnik. DOI: 10.1007/s00502-017-0473-7

[22] Hromada M., Janeckova H., Rehak D.,Slivkova S. and Stuberova D. (2022) *Strengthening Resilience in the Energy Critical Infrastructure: Methodological Overview*, Energies 2022, Vol. 15. Retrieved from https://doi.org/10.3390/en15145276

[23] ISO 22313 (2020): Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

[24] ISO/TS 22317 (2021): Security and resilience — Business continuity management systems — Guidance for business impact analysis

[25] ISO/TS 22318 (2021): Security and resilience — Business continuity management systems — Guidance for supply chain management

[26] ISO/TS 22330 (2018): Security and resilience — Business continuity management systems — Guidance for people aspects of business continuity

[27] ISO 22301 (2019): Security and resilience — Business continuity management systems — Requirements

[28] ISO/IEC 27019:2017: Information technology — Security techniques — Information security controls for the energy utility industry

[29] Iyer A., Prusty A., Saha A. and Thomas R.(2022) *Electric power supply chains: Achieving security, sustainability, and resilience.* Deloitte Insights.

[30] Johnson C. and Wallis T. (2020). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. Retrieved from https://eprints.gla.ac.uk/223565/1/223565.pdf

[31] Kelly T.K., Peerenboom J.P and Rinaldi S.M. (2001) *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine.

[32] Kumar V., Prasad J., Samikannu R. (2018) *A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector*, Int. J. Critical Infrastructures, Vol. 14, No. 2, p.101–119.

[33] Lam W. (2002) *Ensuring Business Continuity*, IT Pro.

[34] Lella, I. et al. (2021). *ENISA THREAT LANDSCAPE 2021.* European Union Agency for Cybersecurity (ENISA), DOI: 10.2824/324797. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[35] Lourenço, M. B., and Marinos, L. (2020). *The year in review: ENISA Threat Landscape.* European Union Agency for Cybersecurity (ENISA), DOI: 10.2824/552242. Retrieved from: https://www.enisa.europa.eu/publications/year-in-review.

[36] Moteff J. and Parfomak P. (2004) *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report for Congress.

[37] NFPA 1600 - Standard on Continuity, Emergency, and Crisis Management (2019). Retrieved from: https://altesafety.com/NFPA_CONTINUITY_EMERGENCY_AND_CRISIS_MANAGEMENT.pdf.

[38] NIST Special Publication (SP) 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems (2021). Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf.

[39] Schmitz-Berndt S. (2023) *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, Journal of Cybersecurity, p. 1–11. Retrieved from https://doi.org/10.1093/cybsec/tyad009

[40] Sievers T. (2021) *Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations*, Int. Cybersecur. Law Rev. (2021) Vol. 2, p. 223–231. Retrieved from https://doi.org/10.1365/s43439-021-00033-8

Annex

Operation of SCADA Systems

A Supervisory Control and Data Acquisition (SCADA) system serves a paramount function within industrial and infrastructure management by facilitating the centralized monitoring and control of dispersed assets across vast geographical expanses. Its primary purpose is to ensure operational efficiency, reliability, and safety through the continuous surveillance of system performance and environmental conditions, thereby enabling timely decision-making and intervention by operators. SCADA systems achieve this through a hierarchical workflow that commences at the data acquisition phase, where field devices and sensors collect real-time data, which is then communicated to Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs), which perform preliminary processing and control tasks tailored to specific local requirements. For more intricate process management, particularly in environments where operations are spatially concentrated, Distributed Control Systems (DCS) are employed, which excel in managing complex, continuous processes by offering refined process control at a localized level, thereby complementing the broader oversight provided by SCADA systems. Both PLCs and DCS contribute to the data ecosystem by funneling processed information to the SCADA system, which then aggregates, analyzes, and presents this data to operators through a centralized interface. This orchestrated interaction between SCADA, DCS, and PLCs forms the backbone of modern industrial control systems, ensuring that energy generation, transmission, and distribution networks operate seamlessly and respond effectively to any arising contingencies.

To summarize, field instruments, such as meters and sensors, initiate the data collection process by transmitting information to PLCs and DCS. Subsequently, this data is conveyed through either wired or wireless networks to SCADA systems, which then present the data on operator interfaces for monitoring and potential intervention. This architecture significantly enhances the ability of operators to oversee and manage systems remotely, offering a level of ease and efficiency not previously attainable with traditional methods, such as the utilization of relay banks, where implementing modifications was a notably intricate and labor-intensive endeavor. The evolution and integration of SCADA systems, which are now accessible via web browsers and are progressing to the form of Industrial Internet of Things (IIoT), underscore the profound impact of digitization on the operational paradigms of industrial systems. This ongoing digital transformation exemplifies the dynamic and increasingly interconnected nature of industrial operations, facilitating unprecedented levels of control, efficiency, and adaptability. Below are the steps in a more consise form:

1. **Data Collection and Preliminary Control:** Field Devices and Sensors Collect data related to energy generation, transmission, distribution, and delivery processes. These devices are the initial source of operational data.

2. **Start Points (Data Sources):**

   - PLCs (Programmable Logic Controllers): Receive data from field devices for initial processing and local control tasks. PLCs can execute automated decisions based on the collected data and send processed information to higher-level systems.

- RTUs (Remote Terminal Units): Similar to PLCs, RTUs collect data from sensors and field devices but are more commonly associated with SCADA systems for remote areas.

3. **Local Process Management:** A DCS (Distributed Control System) receives processed data from PLCs/RTUs for managing local processes close to their operation sites. DCS systems facilitate the fine-tuning of operations and ensure local system stability.

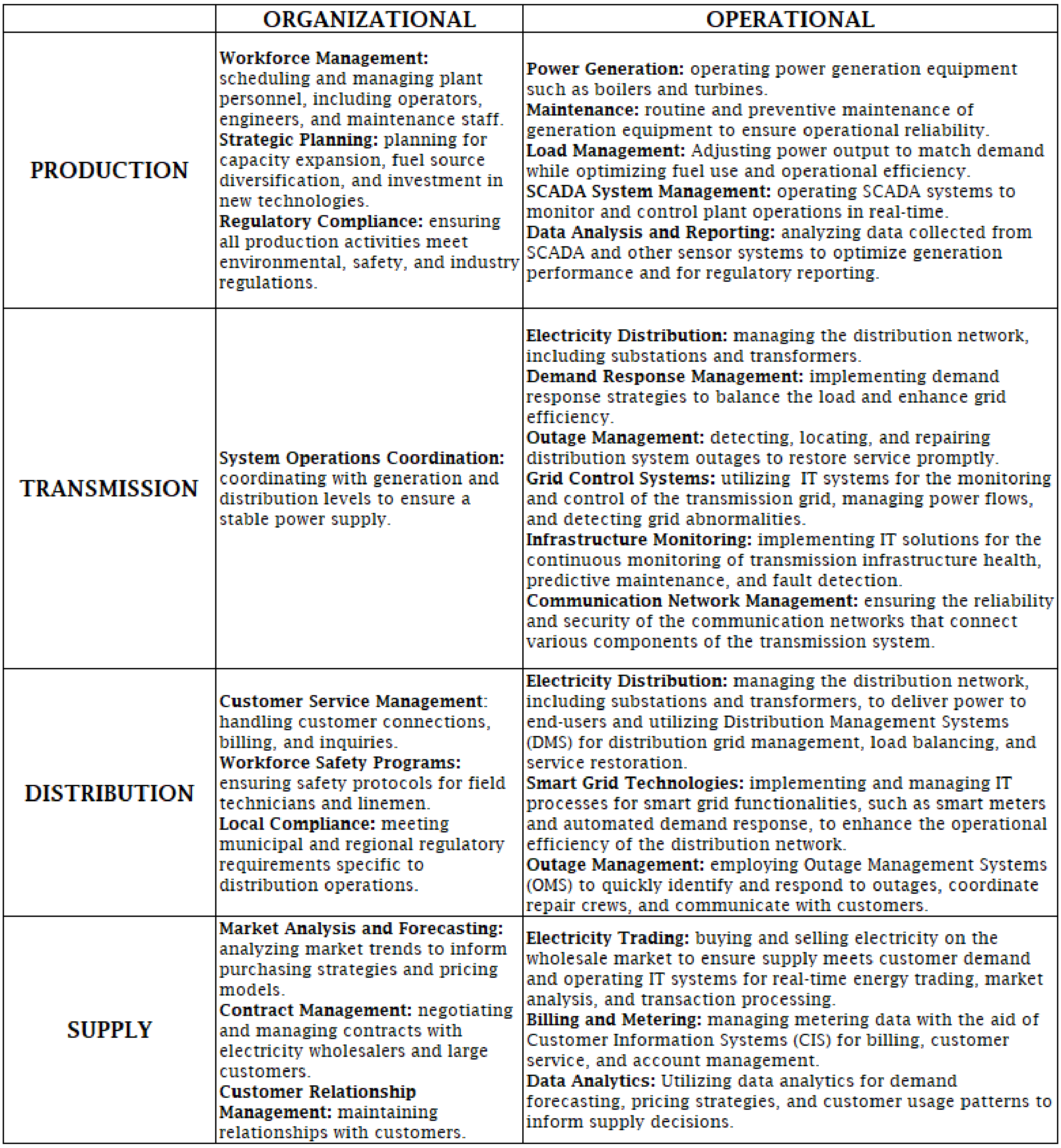
4. **Central Monitoring and Control:** A SCADA system integrates data received from PLCs/RTUs (and directly from field devices in some configurations) for central monitoring and overarching control of the energy system. SCADA systems provide operators with a comprehensive view of the system's status and allow for remote control of operations.

5. **Data Aggregation and Analysis:** MTUs (Master Terminal Units) aggregate data within the SCADA system for further analysis, decision-making, and historical data logging.

6. **Network Infrastructure:** Communication Networks Facilitate the transmission of data between field devices, PLCs/RTUs, DCS, and SCADA systems using various mediums like fiber optics, cables, or RF/microwave communications.

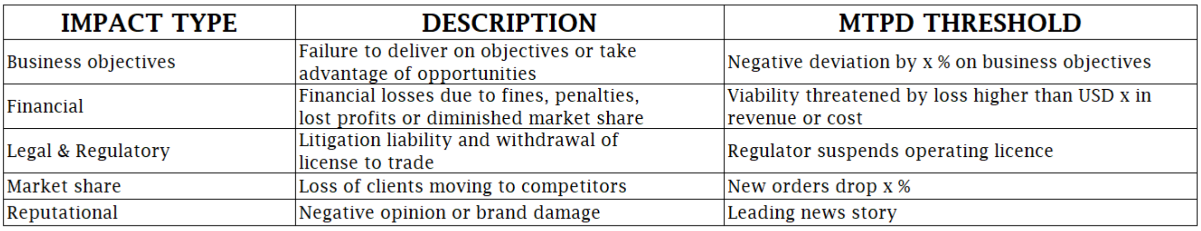
7. **Control Centers:** Servers, workstations, anddisplay systems utilize software for data visualization, state estimation, reporting, and controlling equipment based on data received through the SCADA system.

8. **End Points (Data Utilization):** Operators and decision-makers use the information displayed by SCADA systems for making informed decisions regarding the operation, maintenance, and emergency response of the energy system. This information is available to them through Human Machine Interfaces (HMIs).



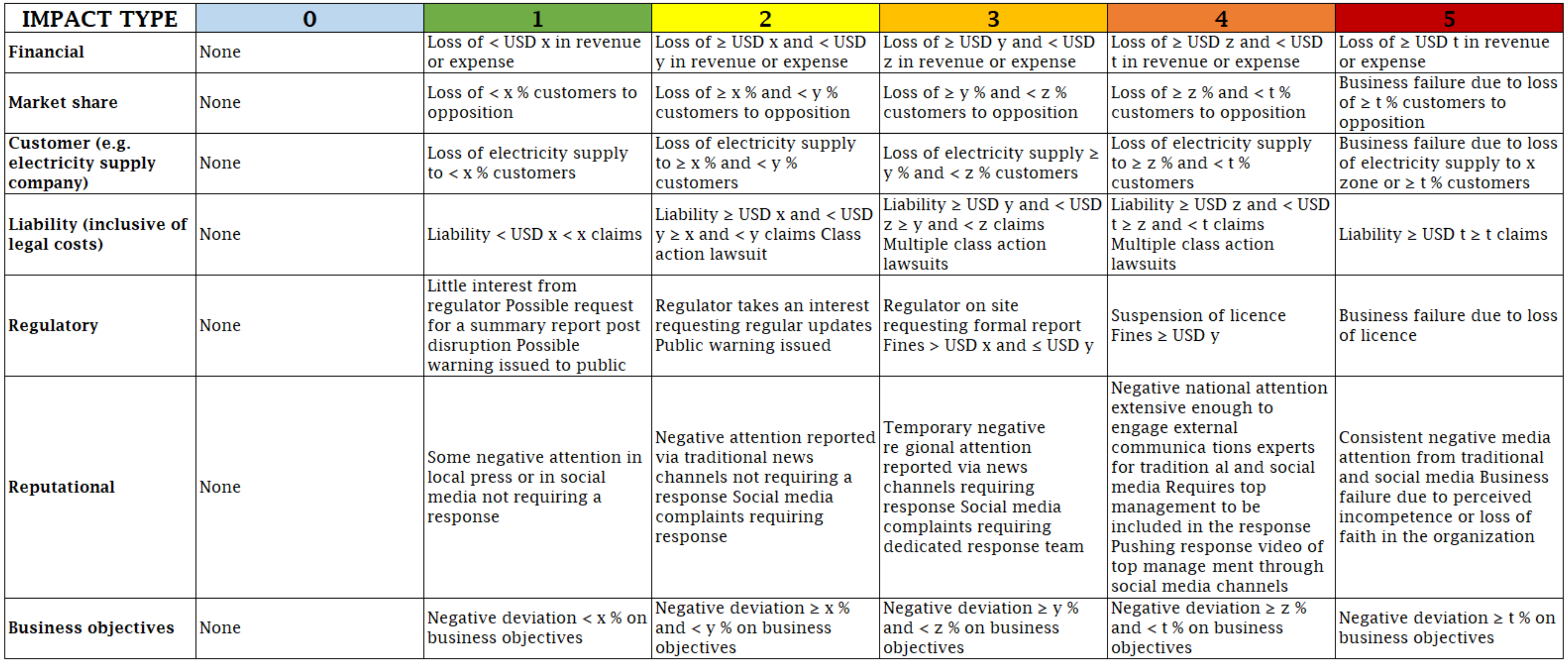
	ORGANIZATIONAL	OPERATIONAL
PRODUCTION	**Workforce Management:** scheduling and managing plant personnel, including operators, engineers, and maintenance staff. **Strategic Planning:** planning for capacity expansion, fuel source diversification, and investment in new technologies. **Regulatory Compliance:** ensuring all production activities meet environmental, safety, and industry regulations.	**Power Generation:** operating power generation equipment such as boilers and turbines. **Maintenance:** routine and preventive maintenance of generation equipment to ensure operational reliability. **Load Management:** Adjusting power output to match demand while optimizing fuel use and operational efficiency. **SCADA System Management:** operating SCADA systems to monitor and control plant operations in real-time. **Data Analysis and Reporting:** analyzing data collected from SCADA and other sensor systems to optimize generation performance and for regulatory reporting.
TRANSMISSION	**System Operations Coordination:** coordinating with generation and distribution levels to ensure a stable power supply.	**Electricity Distribution:** managing the distribution network, including substations and transformers. **Demand Response Management:** implementing demand response strategies to balance the load and enhance grid efficiency. **Outage Management:** detecting, locating, and repairing distribution system outages to restore service promptly. **Grid Control Systems:** utilizing IT systems for the monitoring and control of the transmission grid, managing power flows, and detecting grid abnormalities. **Infrastructure Monitoring:** implementing IT solutions for the continuous monitoring of transmission infrastructure health, predictive maintenance, and fault detection. **Communication Network Management:** ensuring the reliability and security of the communication networks that connect various components of the transmission system.
DISTRIBUTION	**Customer Service Management**: handling customer connections, billing, and inquiries. **Workforce Safety Programs:** ensuring safety protocols for field technicians and linemen. **Local Compliance:** meeting municipal and regional regulatory requirements specific to distribution operations.	**Electricity Distribution:** managing the distribution network, including substations and transformers, to deliver power to end-users and utilizing Distribution Management Systems (DMS) for distribution grid management, load balancing, and service restoration. **Smart Grid Technologies:** implementing and managing IT processes for smart grid functionalities, such as smart meters and automated demand response, to enhance the operational efficiency of the distribution network. **Outage Management:** employing Outage Management Systems (OMS) to quickly identify and respond to outages, coordinate repair crews, and communicate with customers.
SUPPLY	**Market Analysis and Forecasting:** analyzing market trends to inform purchasing strategies and pricing models. **Contract Management:** negotiating and managing contracts with electricity wholesalers and large customers. **Customer Relationship Management:** maintaining relationships with customers.	**Electricity Trading:** buying and selling electricity on the wholesale market to ensure supply meets customer demand and operating IT systems for real-time energy trading, market analysis, and transaction processing. **Billing and Metering:** managing metering data with the aid of Customer Information Systems (CIS) for billing, customer service, and account management. **Data Analytics:** Utilizing data analytics for demand forecasting, pricing strategies, and customer usage patterns to inform supply decisions.

Figure 4: Electricity Sector Operational & Organizational Processes



IMPACT TYPE	DESCRIPTION	MTPD THRESHOLD
Business objectives	Failure to deliver on objectives or take advantage of opportunities	Negative deviation by x % on business objectives
Financial	Financial losses due to fines, penalties, lost profits or diminished market share	Viability threatened by loss higher than USD x in revenue or cost
Legal & Regulatory	Litigation liability and withdrawal of license to trade	Regulator suspends operating licence
Market share	Loss of clients moving to competitors	New orders drop x %
Reputational	Negative opinion or brand damage	Leading news story

Figure 5: ISO 22317 - Types of Impacts



IMPACT TYPE	0	1	2	3	4	5
Financial	None	Loss of < USD x in revenue or expense	Loss of ≥ USD x and < USD y in revenue or expense	Loss of ≥ USD y and < USD z in revenue or expense	Loss of ≥ USD z and < USD t in revenue or expense	Loss of ≥ USD t in revenue or expense
Market share	None	Loss of < x % customers to opposition	Loss of ≥ x % and < y % customers to opposition	Loss of ≥ y % and < z % customers to opposition	Loss of ≥ z % and < t % customers to opposition	Business failure due to loss of ≥ t % customers to opposition
Customer (e.g. electricity supply company)	None	Loss of electricity supply to < x % customers	Loss of electricity supply to ≥ x % and < y % customers	Loss of electricity supply ≥ y % and < z % customers	Loss of electricity supply to ≥ z % and < t % customers	Business failure due to loss of electricity supply to x zone or ≥ t % customers
Liability (inclusive of legal costs)	None	Liability < USD x < x claims	Liability ≥ USD x and < USD y ≥ x and < y claims Class action lawsuit	Liability ≥ USD y and < USD z ≥ y and < z claims Multiple class action lawsuits	Liability ≥ USD z and < USD t ≥ z and < t claims Multiple class action lawsuits	Liability ≥ USD t ≥ t claims
Regulatory	None	Little interest from regulator Possible request for a summary report post disruption Possible warning issued to public	Regulator takes an interest requesting regular updates Public warning issued	Regulator on site requesting formal report Fines > USD x and ≤ USD y	Suspension of licence Fines ≥ USD y	Business failure due to loss of licence
Reputational	None	Some negative attention in local press or in social media not requiring a response	Negative attention reported via traditional news channels not requiring a response Social media complaints requiring response	Temporary negative re gional attention reported via news channels requiring response Social media complaints requiring dedicated response team	Negative national attention extensive enough to engage external communica tions experts for tradition al and social media Requires top management to be included in the response Pushing response video of top manage ment through social media channels	Consistent negative media attention from traditional and social media Business failure due to perceived incompetence or loss of faith in the organization
Business objectives	None	Negative deviation < x % on business objectives	Negative deviation ≥ x % and < y % on business objectives	Negative deviation ≥ y % and < z % on business objectives	Negative deviation ≥ z % and < t % on business objectives	Negative deviation ≥ t % on business objectives

Figure 6: ISO 22317 - Criteria for Severity of Impacts