Guidehouse
Outwit *Complexity*

ENTSO-E - Network Code on Cybersecurity

On January 14, 2022, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced the details of its new cybersecurity code. The Network Code on Cybersecurity (NCCS) is the first network code that will be developed according to the new rules established by the EU directive Article 13 of Regulation 2019/943 on the internal market for electricity. The formal network code development process is expected to be formalized by the European Commission by June 2022 and enter into force by January 2024.

What Does the Code Mean for Utilities?

The network code aims to set a European standard for the cybersecurity of cross-border electricity flows. The code focuses on improving cybersecurity resilience through the enhancement of threat decision, incident reporting. It also proposes various measures to improve cybersecurity resilience that are essential to preserving the continuity of the services you provide.

Guidehouse regulatory compliance and cybersecurity experts have written this whitepaper to give you an overview on the proposed regulations. Details on the Network code can be found here; we've summarized some of the most pressing considerations below into 6 key focus areas.

1. Identify Your Impact Level

It is the responsibility of each cybersecurity ? – National Competent Authority (CS-NCA) to determine if an organization is a high or critical-impact organization. This will be identified within six months after the regulation in enforced, based on an electricity cybersecurity impact index (ECII) developed by ENTSO-E.

Organizations are expected to have established a cybersecurity management system compliant with the NCCS code within 24 months after being notified by the CS-NCA or the National Regulated Authority (NRA)

Additionally, this regulation also applies to those service providers not established in the European Union (EU), but who deliver critical services to organizations within the EU.

2. Conduct A Gap Analysis

One of the most critical tasks for compliance with the NCCS is conducting a gap analysis. This analysis provides a comparison of your current security posture versus the requirements needed in the new directive. This will help you identify areas where vulnerabilities and risks are and determine any gaps.

Develop Recommendations and Roadmap

- Project planning
- Establish data exchange protocols and issue information request
- Establish schedule and interviews
- Review existing cyber security processes, policies, and procedures
- Interview SMEs and key personnel involved on applicable cyber security practices

Develop Recommendations and Roadmap

- Understand cyber security program capabilities
- Identify gaps with cyber security best practices and compliance compared to ISO27001:2018
- Identify areas of improvement associated with people, processes, and tools
- Establish benchmark comparison of findings against industry best practices

Develop Recommendations and Roadmap

- Document overall IT security posture
- Identify recommendations to address compliance and cyber security program gaps
- Develop a prioritized implementation roadmap to address identified gaps
- Identify resource/equipment estimates to implement and sustain recommendations

3. Utilize an established cybersecurity framework

Organizations are tasked to review existing cybersecurity management frameworks or start an implementation plan to have one in place. The network code requires that all organizations to set up an Information Security Management System (ISMS) to manage the cybersecurity risks and the implementation of cybersecurity controls. The ISMS should be designed to ensure the continuous improvement of cybersecurity.

While the network code includes general requirements for an ISMS, mainly derived from the ISO/IEC 27001 standard, the network code does not require that this standard is followed. ISMS based on other standards can be considered if they meet the ISO27001 standard, for example:

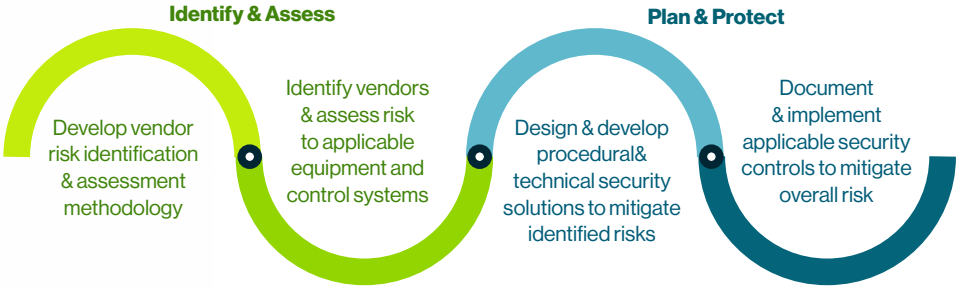
- Conducting internal audits
- Evaluation cyber security performance
- Assign responsibilities
- Demonstrate leadership and executive commitment

ENTSO-E are yet to confirm the minimum cyber security controls that are mandatory for both high and critical risk organizations, and the additional advanced cybersecurity controls for critical risk organizations. These requirements were removed from the network code due to stakeholder feedback and are to be addressed in detail in the Network and information security 2.0 directive (NIS2D) for basic cyber hygiene.

4. Supply Chain Security

There is a great emphasis on supply chain security and resilience, specifically any high or critical assets within your ICT (OT/SCADA/ICS) environment, and associated services: *"all Information and Communication Technology (ICT) products, ICT services and ICT processes inside the high impact and critical impact perimeters"*

As well as external suppliers this will cover any internal teams that provide services e.g., internal IT support teams. Guidehouse utilizes a customized supply chain methodology to help illuminate, identify and manage supply chain risks. We identify critical suppliers, develop risk criteria, conduct assessments, and then propose remediation plans to minimize any business impacts of your supply chain, as highlighted below:



High and critical-impact organizations will be tasked to define cybersecurity procurement requirements for their ICT products, services and processes. ENTSO-E notes that this may require significant effort, and to reduce this burden on originations, and to have harmonized procurement requirements across the EU a reference document will be created by them.

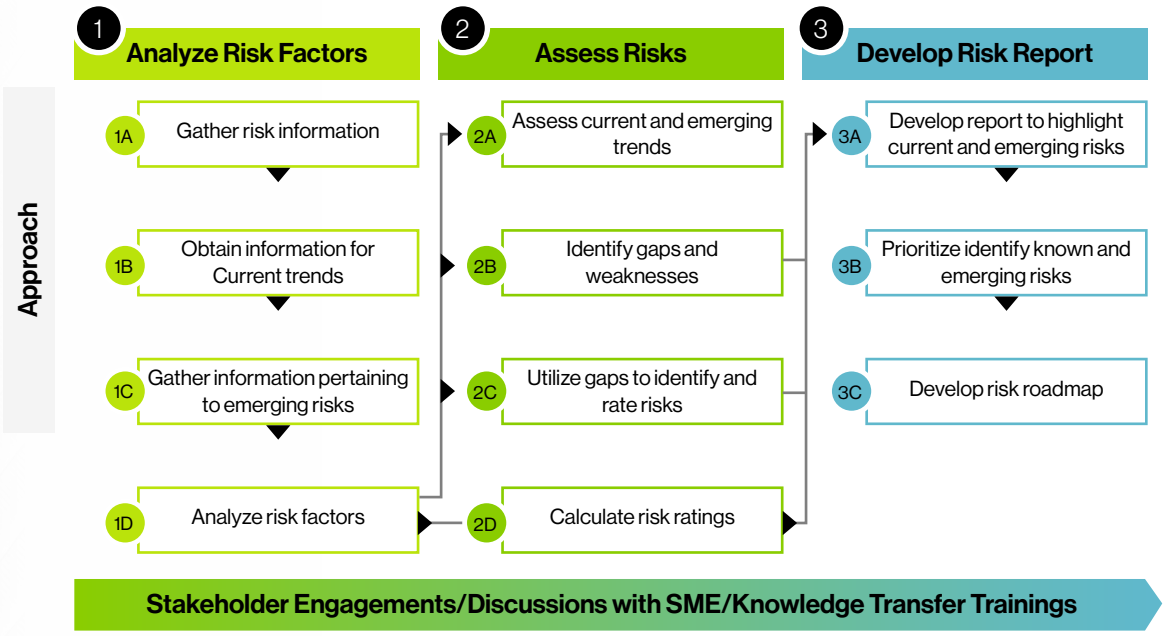
Additionally suppliers will also have additional security controls to adhere to including, providing evidence of implementing security by design in there product development and design, security updates for the lifetime of any products and services they provide, and the right for the customer to audit internal design and development processes. Those classed as critical service providers will have to carry out vulnerability assessments on there products and services and report on any vulnerabilities found, evidence cyber security training, and improve there identity and access management to customers assets they may have access too.

5. Risk assessments

Each member states cybersecurity– National Competent Authority (CS-NCA) is required to carry out its own risk assessment on all high and critical organizations, these included an assessment of your implementation status and plans of the minimum and advanced cybersecurity controls, and a list of security incidents of the previous 3 years.

At an organizational level, the risk assessment is more in-depth in its requirements. As the NCCS aligns to ISO27701, there is a requirement on the cybersecurity risk assessment steps derived from ISO/27005:2018 information security risk management standard, which includes at a minimum: context establishment; cybersecurity risk assessment; risk treatment; and risk acceptance, etc.

Guidehouse's risk assessment methodology takes these requirements into account, as well as considering legacy systems, existing control maturity, and threats actors as part of our assessment.



Each high and critical-impact organization will have to report every 12 months to its CS-NCA on its risk assessment including:

- The list of controls selected for risk treatment
- A list of critical service providers

6. Incident management and response

The NCCS has stricter timelines for sharing information on reportable cybersecurity incidents than the NIS Directive. For reportable incidents, there is a 4-hour time limit to report to its national CSIRT team, and a 24-hour notification for any non-disclosed zero-day vulnerabilities.

Any high or critical assets within your OT/SCADA/ICS environment, will need to be monitored by either an internal or external Cyber Security Operation Center (CSOC), in order to identify and detect intrusions on the network.

In addition to the annual testing of an incident response plan, business continuity plans (BCP) must be tested every 3 years, and any deficiency found in these plans must be remediated with 180 days and a new test will need to be carried out to revalidate the BCP.

Guidehouse
Outwit *Complexity*

Our Company

12,000+ employees

50+ locations globally

Forbes 2019 AMERICA'S BEST MID-SIZE EMPLOYERS — **4** consecutive years on Forbes Top Employers

2021 Military Friendly® Program

GovCon 2020 Contractor of the Year, Over $300 Million

12 #1 Rankings — KLAS RESEARCH

Malcolm Baldrige National Quality Award 2014 Award Recipient

Malcolm Baldrige National Quality Award Recipient

Modern Healthcare 2021 BY THE NUMBERS — #3 Guidehouse — Largest Healthcare Management Consulting Firms

Our People

33 languages fluently spoken

46% hold professional certifications

38% have advanced degrees

Commitment to Inclusion, Diversity and Belonging

37% racially diverse

11 consecutive perfect scores with HRC

6 generations of professionals

BEST PLACES TO WORK 2022 for LGBTQ+ Equality — 100% CORPORATE EQUALITY INDEX

49% female
51% male

DiversityInc — Great Place to Work

7 employee affinity groups

DiversityInc TOP 50 COMPANIES FOR DIVERSITY NOTEWORTHY 2021

Great Place To Work. Certified AUG 2021-AUG 2022 USA

5% Veteran and Active Duty

Healthcare: **7** of the top 10 hospital systems (by Member Hospital Beds)*

Financial Services: **8** of the 10 largest U.S. banks

Life Sciences: **38** of the top 50 pharmaceutical companies**

Energy: **60** of the world's largest electric and gas utilities***

Public Sector: **15** (all) executive departments of the U.S. Federal Government

State & Local Government: **30** out of 50 States

Guidehouse's Energy, Sustainability & Infrastructure Segment

With more than 900 consultants, Guidehouse's global Energy, Sustainability, and Infrastructure segment is the strongest in the industry. We are the go-to partner for leaders creating sustainable, resilient communities and infrastructure, serving as trusted advisors to utilities and energy companies, large corporations, investors, NGOs, and the public sector. We've solved big challenges with the world's 60 largest electric, water, and gas utilities; the 20 largest independent power generators; five of the 10 largest oil and gas majors; the 20 largest gas distribution and pipeline companies; European governments; and the US federal government's civilian agencies involved in the country's land, resources, and infrastructure. We combine our passion, expertise, and industry relationships to forge a resilient path toward sustainability for our clients. We turn vision into action by leading and derisking the execution of big ideas and driving outcomes for our clients that enable them to reach their ambitions through transformation. For more information, visit **www.guidehouse.com/esi**.

The Guidehouse Advantage

Guidehouse's Cybersecurity team and our Energy, Sustainability, and Infrastructure team promote and foster the effective security practices integrated with operational and compliance goals. Our deep energy industry experience, combined with a comprehensive understanding of the technology, strategy, and security interventions needed across the energy sector's IT and OT assets, positions us to start fast and succeed immediately. Our experts help energy companies and utilities conduct cybersecurity assessments, harden security, streamline compliance, and increase resilience — so they are prepared for any threats the future has in store for them.

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 12,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit **www.guidehouse.com**

For more information contact:

Barry Coatesworth
Director
Barry.coatesworth@guidehouse.com

Chris Luras
Partner, Energy—Security & Compliance
chris.luras@guidehouse.com

Keshav Sarin
Director, Energy—Security & Compliance
keshav.sarin@guidehouse.com