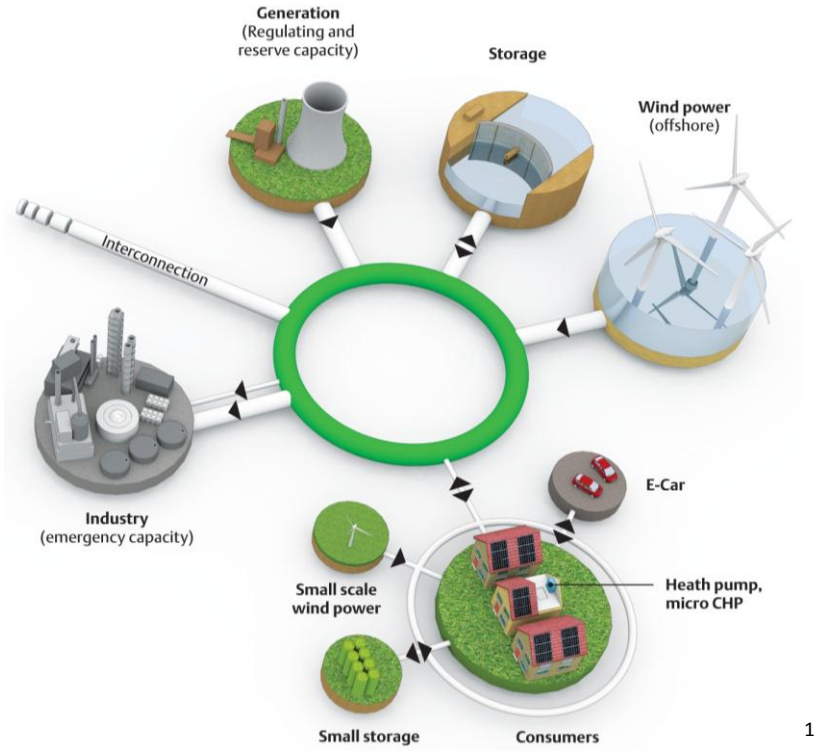


[1]

Appropriate security measures for smart grids

Guidelines to assess the sophistication of security measures implementation

[2012-12-06]

[1] *Copyright TenneT*

DOCUMENT HISTORY

Date	Version	Modification	Author
21.09.2012	1.0	Preliminary draft structure	Deloitte (Dan Cimpean, Pedro Cano, Fernando García)
01.10.2012	1.1	Comments on the preliminary draft	ENISA (Konstantinos Moulinos, Thomas Haeberlen)
11.10.2012	1.2	Updated Version	Deloitte (Dan Cimpean, Pedro Cano, Fernando García)
11.10.2012	1.3	Updated Version	Deloitte (Dan Cimpean, Pedro Cano)
11.10.2012	1.4	Updated Version	Deloitte (Dan Cimpean, Pedro Cano, Fernando García)
22.10.2012	1.5	Updated Version	Deloitte (Dan Cimpean, Pedro Cano)
23.10.2012	1.5.1	Comments on the draft	ENISA (Konstantinos Moulinos, Thomas Haeberlen)
22.11.2012	1.6	Updated Version	Deloitte (Dan Cimpean, Pedro Cano; Fernando García)
06.12.2012	1.7	Final Version	Deloitte (Dan Cimpean, Pedro Cano; Fernando García)

Contributors to this report

ENISA would like to recognise the contribution of the Deloitte team members that prepared this report in collaboration with and on behalf of ENISA:

- Dan Cimpean;
- Pedro Cano Bernaldo de Quirós;
- Fernando García Gutiérrez.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at http://www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on Critical Information Infrastructure Protection, please use the following details:

- E-mail: resilience@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to Minimum Security Measures for Smart Grids, please use the following details:

- **Dr Konstantinos MOULINOS,** Expert in Network & Information Security - Resilience and CIIP, European Network and Information Security Agency - ENISA
- Address: Vassilika Vouton, GR-70013 Heraklion, Greece
- Email: resilience@enisa.europa.eu

Follow us on

Facebook: http://www.facebook.com/ENISAEUAGENCY

Twitter: https://twitter.com/enisa_eu

LinkedIn: http://www.linkedin.com/company/european-network-and-information-security-agency-enisa

Youtube: https://www.youtube.com/user/ENISAvideos

RSS feeds: http://www.enisa.europa.eu/front-page/RSS

Contents

Preface 6
1 Introduction 7
1.1 Background 7
1.2 Scope 9
1.3 Target audience 9
1.4 Development approach 9
1.5 Document overview 10
2 Approach to identifying appropriate security measures 12
2.1 Structure 12
2.2 The role of risk assessment 15
2.3 Lessons identified 17
2.4 Domains 19
3 Appropriate security measures 20
3.1 Domain 1: Security governance & risk management 20
3.2 Domain 2: 2. Management of third parties 22
3.3 Domain 3: Secure lifecycle process for smart grid components/systems and operating procedures 23
3.4 Domain 4: Personnel security, awareness and training 26
3.5 Domain 5: Incident response & information knowledge sharing 28
3.6 Domain 6: Audit and accountability 30
3.7 Domain 7: Continuity of operations 31
3.8 Domain 8: Physical security 32
3.9 Domain 9: Information systems security 33
3.10 Domain 10: Network security 35
4 Sophistication levels 37
4.1 Domain 1: Security governance & risk management 37
4.2 Domain 2: Management of third parties 41
4.3 Domain 3: Secure lifecycle process for smart grid components/systems and operating procedures 43
4.4 Domain 4: Personnel security, awareness and training 49

4.5 Domain 5: Incident response & information knowledge sharing 52
4.6 Domain 6: Audit and accountability 55
4.7 Domain 7: Continuity of operations 57
4.8 Domain 8: Physical security 60
4.9 Domain 9: Information systems security 62
4.10 Domain 10: Network security 67
5 Catalogue of security measures 70
6 Mapping with ISO/IEC 27002, NISTIR 7628 and ISO/IEC TR 27019 71
Annex I - Glossary 79
Annex II – References 81

Preface

The development of an efficient, reliable and sustainable environment for the production and distribution of energy in the future is linked to the use of smart grids. Various market drivers, regulatory or standardisation initiatives have appeared or gained importance as tools to help involved stakeholders to be prepared against smart grids security vulnerabilities and attacks. The perception and the approach taken on this topic differ among stakeholders. This underlines the importance of the stakeholder's alignment on the key aspects related to the smart grid security.

The European Network and Information Security Agency (ENISA) has decided to further investigate the challenges of ensuring an adequate smart grid protection in Europe, in order to help smart grid providers to improve the security and the resilience of their infrastructures and services. Defining a common approach to addressing smart grid cyber security measures will help achieve this.

This technical document provides guidance to smart grid stakeholders by providing a set of minimum security measures which might help in improving the minimum level of their cyber security services. The proposed security measures are organised into three (3) sophistication levels and ten (10) domains, namely:

1. Security governance & risk management;
2. Management of third parties;
3. Secure lifecycle process for smart grid components/systems and operating procedures;
4. Personnel security, awareness and training;
5. Incident response & information knowledge sharing;
6. Audit and accountability;
7. Continuity of operations;
8. Physical security;
9. Information systems security; and
10. Network security.

The adoption of a particular set of security measures needs the consensus and cooperation of various stakeholders in the smart grid community. A coordination initiative could allow a common and generally accepted approach to addressing smart grid security issues. Moreover, the development of a common approach to addressing smart grid cyber security measures will help not only regulators by harmonising the complex smart grid's environment but also by providing incentives to other involved stakeholders to continuously strive for the improvement of their cyber security.

1 Introduction

This document describes a set of security measures which are considered to be appropriate for smart grids. ENISA issued this report in order to assist the Member States and smart grid stakeholders in providing a framework/measurement tool that could be used for:

- Aligning the varying levels of security and resilience of the market operators with a consistent minimum framework;
- Providing an indication of a minimum level of security and resilience in the Member States with regards to the smart grids, thereby avoiding the creation of the "weakest link";
- Ensuring a minimum level of harmonisation on security and resilience requirements for smart grids across Member States and thus reducing compliance and operational costs;
- Setting the basis for a minimum auditable framework of controls across Europe;
- Facilitating the establishment of common preparedness, recovery and response measures and pave the way for mutual aid assistance across operators during crisis;
- Contributing to achieve an adequate level of transparency in the internal market.

1.1 Background

European energy targets

The European Union has established very ambitious objectives for 2020: 20% of renewable energy penetration, 20% of CO_2 emissions reduction and an increase of 20% in energy efficiency. A key issue, in order to achieve these targets, is the effective integration of the distributed renewable energy generation into current and future electricity grids (smart grids): not only innovative technical solutions are required, but also new suitable regulatory and economic schemes at European scale.

In order to achieve the defined objectives and the future vision of the energy market in Europe, an increase in the efficiency, reliability, quality and safety of the European electricity system is needed. In this context, the Strategic Energy Technology Plan (SET Plan) establishes the key goals focused on the overall energy research effort in Europe.

Until recently, the installed capacity of distributed generation in Europe was too low to be a critical issue in the management of the electricity distribution network. The new advances imply an increasing use of the desirable renewable energy sources and, therefore, progressively lower costs per installed power capacity.

Technical advances, environmental improvement and control wished by citizens and the European Union's commitment to the Kyoto Protocol are drivers that have positioned smart grids as an alternative to manage the increasing distributed generation and the involved challenges.

Smart grids security

Smart grids have been defined by the European Smart Grid Task Force (set up by the European Commission at the end of 2009) as "*electricity networks that can efficiently integrate the behaviour and actions of all users connected to it - generators, consumers and those that do both - in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply*".

Smart grids have an essential role in the process concerning the integration of variable distributed resources in the electricity networks (key driver to get 2020 targets) and providing a user-oriented service, supporting the achievement of these targets.

Current developments on the power networks, such as digital communication between supplier and consumer, intelligent metering and monitoring systems, will allow smart grids to improve the control over electricity consumption and distribution substantially to the benefit of consumers, electricity suppliers and grid operators.

Moreover, not only advanced Information and Communication Technologies (ICT) are at the core of an effective smart grid implementation. Also industrial control systems (ICS) and related operational technology (OT) need to be taken into account. All processes across the whole value chain are heavily based on these infrastructures and technologies. Smart grids give clear advantages and benefits to the whole society, but the dependency on ICT components (e.g. computer networks, intelligent devices, etc.), ICS (e.g. supervisory control and data acquisition systems, distributed control system, etc.), OT (e.g. firmware, operating systems, etc.) and the internet makes our society more vulnerable to malicious attacks with potentially devastating results on smart grids. This can happen in particular because vulnerabilities in smart grid related communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants.

The Commission published the "Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment" on March 1st of 2011, in which it defined a standardisation mandate to support European Smart Grid deployment. This document is a starting point for the normalisation of energy interoperability and will enable or facilitate the implementation in Europe of the different high level smart grid services and functionalities.

Regarding security issues, the mandate states *"A secure and robust energy network is essential for the continuous improvement and industrious operation of the European energy markets. This will only be possible if the associated information and communication networks are secure and robust. It is also essential to maintain data and system security and to respect the rights of end consumers as well as the fundamental rights and freedoms of natural persons."*

Moreover, the "Commission Recommendation of 9 March 2012, on preparations for the roll-out of smart metering systems , (2012/148/EU)" in its article 27 notes that "*Member States should ensure that network operators identify security risks and the appropriate security*

measures to guarantee the adequate level of security and resilience of the smart metering systems. In this regard, network operators, in cooperation with national competent authorities and civil society organisations, should apply existing standards, guidelines and schemes and where not available develop a new one. Relevant guidelines published by the European Network Information and Security Agency (ENISA) should also be taken into account."

1.2 Scope

This technical guidance addresses smart grid networks[2] and services which are critical and whose malfunctioning would have a significant impact on society. Data privacy issues, however, are considered out of scope of this document.

1.3 Target audience

The present document is focused on the following actors:

- Legislator(s) and the regulator(s) at various levels (EU, Member State);
- Distribution system operators (DSO);
- Transmission system operators (TSO);
- Bulk generation and 'bulk' renewables (e.g., wind farm) operators;
- Third party service and solutions providers;
- Energy traders;
- Third party financial services;
- Smart Grid equipment manufacturers;
- Prosumers[3].

1.4 Development approach

The first phase of the project was based on a stock taking exercise of existing frameworks and standards related to smart grid security practices - completed with an extensive desk research activity. This stock taking involved the following categories of stakeholders:

- Regulators and policy makers;
- Smart Grid Operators;
- Standardisation Bodies (e.g. ETSI, NIST, IEC, ISO, etc.);
- Security solutions providers;
- Smart Grid manufacturers;
- Academia, R&D;
- Public bodies in the Member States involved in Smart Grid cyber security.

---

[2] *Covering today's grid , their continuous further development and even the visionary future holistic smart grid*

[3] *Prosumers: combination of the roles of consumer and producer. In the energy context is the combination of the roles generator and energy user. (see Annex I – Glossary)*

The information obtained during this phase was complemented with other sources and reports that have been considered relevant for the purpose of the study. The following key information sources have been identified:

- Meeting minutes of the stock taking exercise that contains the relevant opinion from the experts;
- Desktop research activity that identified the existing practices and standards related to cyber security that could be used to measure the security maturity level (including current European initiatives for securing smart grids);
- Reports from governmental agencies providing information regarding operational capabilities for defence of control system environments against emerging cyber threats (e.g. EUROSCSIE, CPNI.UK and CPNI.NL);
- Research documents about various aspects of information security from trusted and recognized entities (e.g. SANS);
- Findings from the Expert Group on the security and resilience of communication networks and information systems for Smart Grids;
- The U.S. Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

Using as a starting point the above mentioned sources, a draft conceptual approach to identifying minimum security measures for smart grids was defined. This approach will help policy makers and energy players to reach alignment on different level of security in smart grid related infrastructures and processes (fig 1). Then, the security measures identified and grouped in domains.

The first draft document, containing both the approach and the measures, was shared for comments with different experts for a predefined consultation time. A new updated version of the document, containing most of the received comments, was presented to the stakeholders in a validation workshop held in Brussels. The final version of the document was published by ENISA at the end of December 2012.

1.5 Document overview

In order to reach the objectives described above, the report has been structured in the following sections:

- **Chapter 1 – Introduction.** This chapter contains an introduction to the smart grid context and the motivation for the study. Moreover, the terminology and methodology used during the study are also described;
- **Chapter 2 – Appropriate security measures.** In this chapter the process used to derive the specific security measures for the smart grid security is described. Moreover, the chapter presents the different domains and the related appropriate security measures selected in the smart grid context;

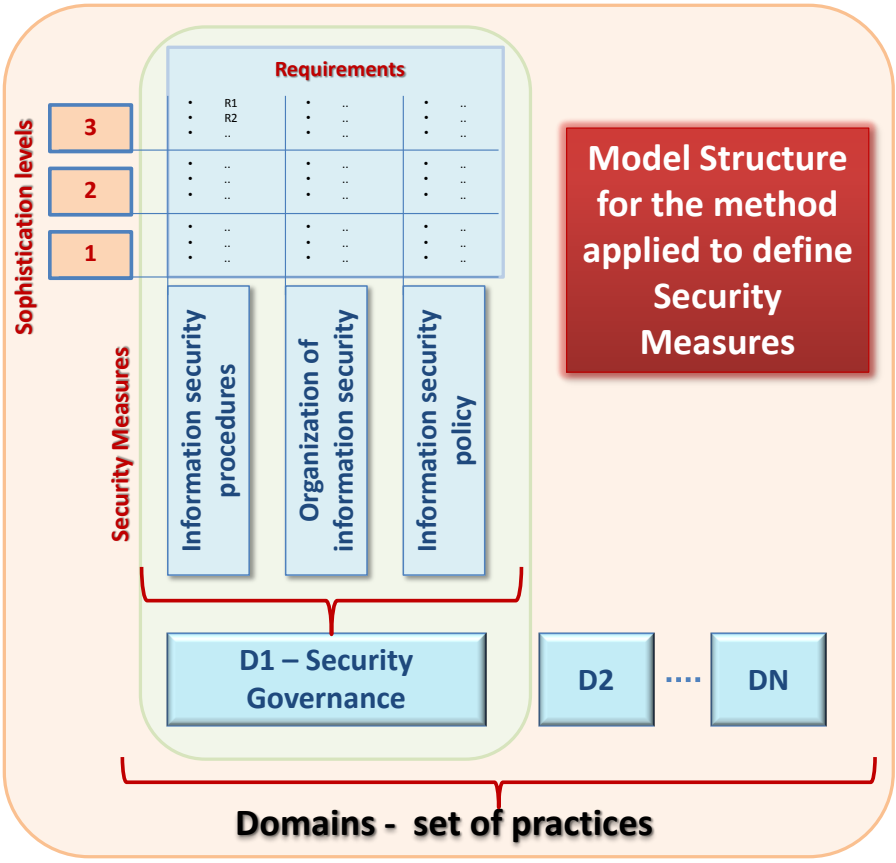
- **Chapter 3 – Sophistication levels.** This chapter contains the identified lists of security measures and related evidence classified within the defined sophistication levels for each domain;
- **Chapter 4 – Catalogue of appropriate security measures.** This chapter contains a table with the defined security measures;
- **Chapter 5 – Mapping with ISO/IEC-27002, NISTIR-7628 and ISO/IEC TR 27019.** This chapter contains a table which represents the relationships between the defined security measures and the standards ISO/IEC-27002, NISTIR-7628 and ISO/IEC TR 27019;
- **Annex I – Glossary.** A set of terms and definitions;
- **Annex II – References.** List of relevant bibliography used in the study.

2 Approach to identifying appropriate security measures

2.1 Structure

The set of smart grid security measures is organised into domains and sophistication levels. This is reflected in the following matrix where the columns are the domains and the rows are the sophistication levels:

Figure 1 – Conceptual model of the approach



The measures are grouped in domains in order (a) to allow the reader to better identify possible security deficiencies and (b) to provide data and high-level guidance that can be used to predict the effectiveness of the proposed domains.

As example:

- Security governance & risk management domain.

Security governance & risk management	Information security policy Organisation of information security Information security procedures Risk management methodology Risk assessment Risk treatment plan

Each identified security measure can be implemented at different levels of sophistication. Each level contains the practices to assess the adequacy of the design and evidence that should be provided in order to check the effective implementation of the security practice. These levels are described as follows:

Sophistication level	Description
1	The security measure is implemented in an early stage (not advanced). Security goals are being achieved to some extent.
2	The security measure is implemented according to industry standards across a large part of the organization. Security goals are being achieved and their effectiveness sometimes (ad-hoc) reviewed.
3	The security measure is implemented in an advanced way, and monitored and tested continuously. The security measure is reviewed on a structural basis, and updated if necessary to support business goals in the best possible fashion. Exercises and tests are organized to check the effectiveness of the measure.

Sophistication levels are applied independently to each domain (Figure 2). As a result, a smart grid provider may receive different sophistication ratings for different domains. It is important to realise that the sophistication levels that are applicable to a given organisation depend on its specific characteristics such as its size or the services provided. For example, for a provider with only 5 employees it may be unnecessary to have a security policy that is fully aligned with best practice industry standards, or to have a documented formal procedure for hiring personnel.

The practices that complete each sophistication level are selected from relevant standards, guidelines and frameworks which have been identified during the stock taking exercise. The practices have been selected from the following key documents:

- NISTIR (National Institute of Standards and Technology Internal Report) 7628: Guidelines for Smart Grid Cyber Security;
- ISO/IEC (International Organization for Standardization) 27002: Information technology —Security techniques — Code of practice for information security management;

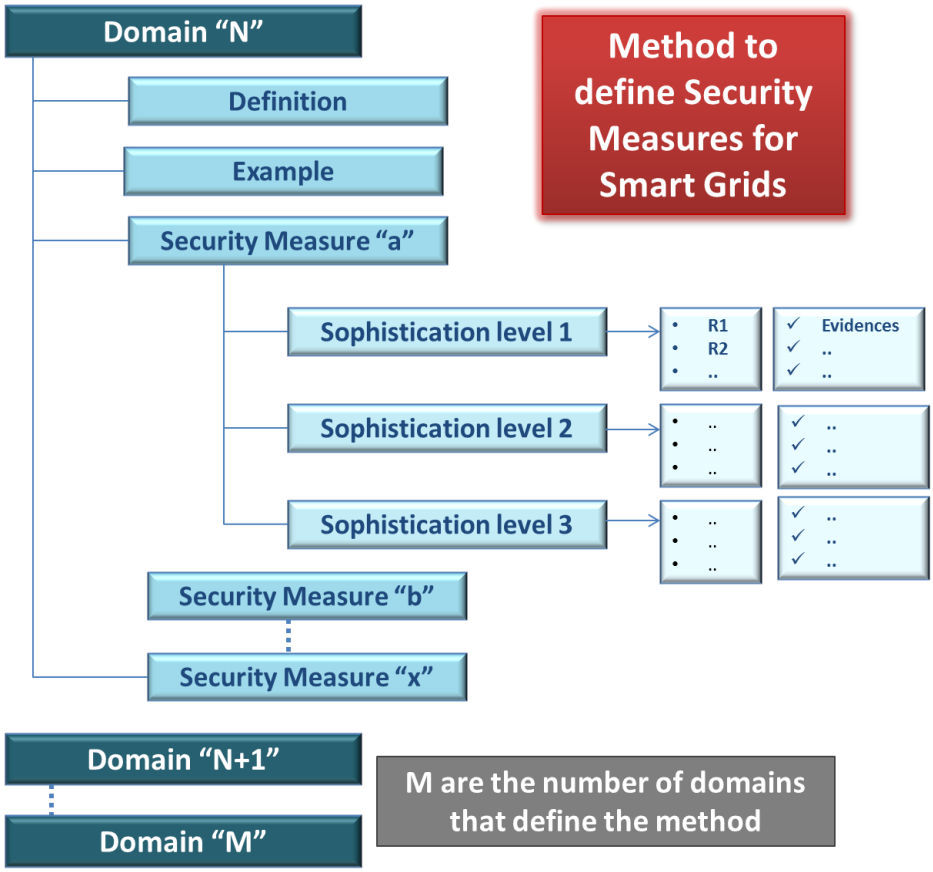
- ISO/IEC (International Organization for Standardization) DIS 27036-2, Information technology – Security techniques – Information security for supplier relationships - Part 2: Requirements;
- ISO/IEC 27011: Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002;
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection);
- IEC (International Electrotechnical Commission) 62443: Technical Specification - Industrial Communication Networks - Network and System Security;
- IEC (International Electrotechnical Commission) 62351: Power Systems Management and Associated Information Exchange – Data And Communications Security;
- ISO/IEC TR (Technical Report) 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry;
- BDEW (BDEW Bundesverband der Energie- und Wasserwirtschaft) - White Paper Requirements for Secure Control and Telecommunication Systems.

As example:

- Information security policy security measures.

SM 1.1 Information security policy The provider shall establish and maintain an appropriate information security policy.		
Level	**Practices**	**Evidence**
1	❖ Minimum security activities on the smart grid information system are performed by the organisation.	✓ Documented security procedures that address the minimum security activities.
2	❖ An information security policy that addresses a secure and reliable energy supply and legal and regulatory requirements is available and approved by management. ❖ Employees are aware of the existence and behave accordingly.	✓ Approved information security policy covering most aspects of security containing at least: o Scope of the information security policy; o Applicable laws and regulations; o Security objectives; o Management commitment with the security policy. ✓ Proof of the information security policy communication among staff. ✓ The information security policy is easy accessible for staff.
3	❖ The information security policy is regularly reviewed[4] at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	✓ Last planned review has been done according with the review process. ✓ Records of the management review. ✓ Meeting minutes of review sessions.

Figure 2 - Overview of the common approach to addressing smart grid cyber security measures



2.2 The role of risk assessment

Organisations wishing to establish, implement, operate, monitor and continuously maintain and improve an appropriate level of smart grid security, must also carefully and continuously consider and assess the actual level of preparedness and the related security risks they face.

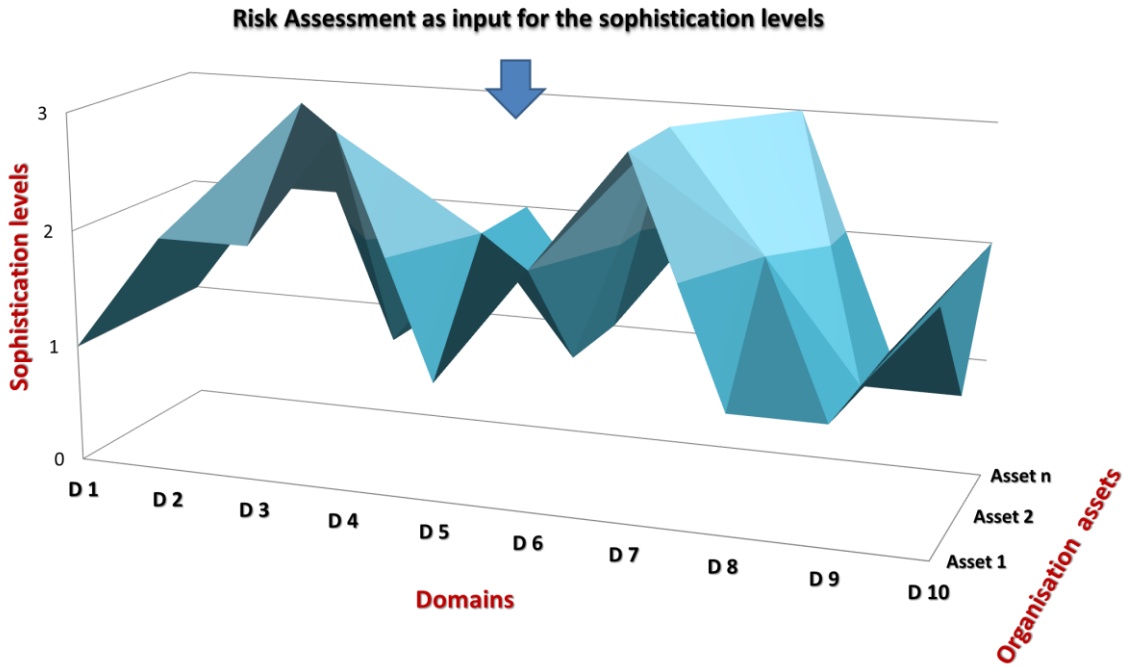
A risk assessment should be performed throughout the system life cycle: during requirements definition, procurement, control definition and configuration, system operations, and system close-out.

A "Risk Assessment" (RA) would be, in this context, an important step to be performed before deciding the required sophistication levels needed by the smart grid organisation. The extent and granularity of the Risk Assessment should take into account several factors such as the size of the organisation, the implementation cost of the measures etc.

The risk assessment allows the smart grid system designer to define a threshold for the minimum acceptance level before the establishment of a risk value and to perform the risk assessment for the assets in scope. Therefore, a risk assessment is a key preliminary step that should be conducted in order to understand what risk level is appropriate/acceptable for each

organisation before deciding upon the required sophistication levels needed by the smart grid organisation (Figure 3):

Figure 3 - The risk assessment is useful input for deciding on the sophistication levels needed



The organisation should select specific controls, measures and sophistication levels by considering and effectively using the results of the risk assessment. This way, the proposed smart grid security measures could be considered as an appropriate benchmark enabling the security managers to determine which specific aspects of security require attention and priority within their respective organisations.

Establishing a security benchmark within a context that has been defined by smart grid experts is considered to be a successful formula, because such a benchmark can be properly focused on smart grid specific security issues. Such benchmark can complement the outcome of the risk assessment and provide an additional input for defining and selecting the specific controls, measures and sophistication levels for smart grid security.

The above-described proposed approach is aligned with general risk management good practices – and therefore will help create synergies between the risk management and the security efforts of the smart grid organisation. In contrast with a compliance based approach, this approach is considered to be more pragmatic and efficient. Moreover, the proposed approach is considered to be more powerful because it takes into consideration the specific characteristics of the smart grid organisation. Therefore, it can be applied to a wide range of smart grid organizations independently of their size or maturity.

The use of sophistication levels allows the definition of different quality requirements each measure. This approach is different from a maturity level approach because, in practice, an organisation will probably not have all its measures developed to the same level of maturity.

The identification of a suitable risk assessment methodology for smart grid establishments is beyond the scope of this report; therefore it has not been described in detail. Only the relevance and usefulness of performing a suitable risk assessment, before deciding the required sophistication levels, was highlighted. For the interested reader, a detailed description of different risk assessment methodologies for the energy sector can be found on the document "Common areas of Risk Assessment Methodologies"[4] by EURACOM (European Risk Assessment and Contingency planning Methodologies for interconnected energy networks).

2.3 Lessons identified

The following key conclusions have been drawn from the analysis of the above mentioned sources:

- The **reliability** and **resilience** of the energy supply chain are critical factors because the smart grid is considered as a single interconnected system with a potential high impact in case of failure;
- There is a considerable number of legacy systems present in almost all smart grid environments. One of the key security challenges with legacy systems is related to the **deployment of security patches** because in some cases it is not possible to install the patches or remove known vulnerabilities;
- As required in every sound information security management system all key involved risks and their mitigating controls must be covered by a regular **internal/external audit process** intended to provide independent assurance on the adequacy of these controls;
- Sharing relevant information between all smart grid organisations will make the **awareness on vulnerabilities and on possible consequences** transparent to all;
- Manufactures are also responsible for contributing to the security of the smart grid (via the involved equipment /devices / components embedded). For instance, it is important to highlight the risks involved by the use of **default configurations** with weak passwords or with unnecessary services enabled;
- An adequate **risk assessment process** is necessary in order to select the adequate security controls for the smart grid organisation while designing the overall architecture and the component specification;

[4] *The document can be download from: http://www.eos-eu.com/?Page=euracom*

- The **security of the smart grid** should be taken into account at an early stage in order to allow set security requirements at planning or development stage at the latest;
- One of the most important objectives of the security infrastructure protecting the smart grid is the **prevention/detection as well as the response against cyber events and/or cyber incidents** before there is significant power system impact;
- Smart grid security is, in general, **poorly integrated with the organisational security or the security management process**; therefore the definition of specific smart grid security requirements might be not aligned with the overall business requirements;
- Focus on **cryptography, privacy, policies and performance** criteria around application security and **threat and vulnerability management** requires significant attention because most smart grid stakeholders still have little experience in these areas;
- As several smart grid activity domains can be identified, there are multiple **actors that participate in the smart grid value chain** (operational smart grid) – inherently this creates complexity in approaching the overall smart grid security challenges;
- The smart grid includes the deployment of multiple interconnected systems and devices; therefore **interoperability is critical**;
- **Security metrics** are a very active research field (when considering smart grids) but solid outcomes have not been achieved yet;
- A skills gap exists between enterprise IT engineers and SCADA engineers with respect to the special information security requirements in the power domain. Therefore, it is necessary to implement specific **training for people** that will be involved on the power domain environment;
- A very important consideration is **designing a proper security of the smart grid network** from the early stages; this way high costs of redesign will be avoided;
- **Physical security aspects** should address the protection of smart grid devices located in the organisation's premises as well as outside of the organisation's own grounds or premises (for example smart grid devices physically located in areas that are the responsibility of other utility providers);
- The necessity of an adequate **identification and authentication process** was acknowledged as one of the most relevant security control aspects in the view of the access to the smart grid;
- Addressing cyber security of smart grids requires the proper **identification of key dependencies** between the ICT-infrastructures and electricity grids, and of all other relevant smart grid assets;
- There is a need to establish a **common procurement language** and/or standard for a base level of security of the smart grid components and services in collaboration with private and public asset owners, vendors and regulators.

These findings have been used as a basis for the definition of the domains.

2.4 Domains

The identified domains cover all the relevant topics noted by the experts and by the additional information sources, namely:

1. **Security governance & risk management:** this domain covers the security measures that should been taken into consideration in order to facilitate a proper implementation and/or alignment with the security culture on smart grid stakeholders;
2. **Management of third parties:** this domain covers the security measures related to the interaction with third parties, so that the smart grid operator can reach a true and sustainable integration to the smart grid as a whole;
3. **Secure lifecycle process for smart grid components/systems and operating procedures:** this domain covers activities and procedures related to the secure operation, configuration, maintenance, and disposal of the smart grid components and systems. Therefore, the security measures included in this domain take into consideration among other things the proper configuration of the smart grid information systems and components or its change management procedures;
4. **Personnel security, awareness and training:** this domain ensures that employees of an organisation running a smart grid receive adequate training to perform reliable operations on the smart grid;
5. **Incident response & information knowledge sharing:** this domain covers the possible security threats, vulnerabilities, and incidents affecting smart grids in order to provide an effective response in case of a potential disruption or incident;
6. **Audit and accountability:** this domain covers the implementation of an audit and accountability policy and associated controls in order to verify compliance with energy and smart grid specific legal requirements and organisation policies;
7. **Continuity of operations:** this domain ensures the basic functions of the smart grid under a wide range of circumstances including hazards, threats and unexpected events;
8. **Physical security:** this domain covers the physical protection requirements for the smart grid assets;
9. **Information systems security:** this domain covers the definition of requirements to protect the information managed by the smart grid information systems using different technologies like firewalls, antivirus, intrusion detection and etc.;
10. **Network security:** this domain covers the design and implementation of requirements that protect the established communication channels among the smart grid information system and the segmentation between business and industrial networks.

3 Appropriate security measures

3.1 Domain 1: Security governance & risk management

Control Objective: The provider has established and maintains a security governance program that directs and controls the smart grid information security. It provides strategic direction, ensures objectives are achieved, cyber security risk aspects regarding the smart grid systems and components have been fully addressed, uses organisational resources responsibly, and monitors the success or failure of the security programme. It should be noted that the programme should identify not only the internal risks but also risks coming from ICT and energy supply chain as appropriate.

ID	SM 1.1
Measure	Information security policy.
Definition	The provider should establish and maintain an appropriate information security policy.
Example	[From ISO/IEC 27002 - 5.1.1 Information security policy document] An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. [From IEC 62443 - 4.3.2.6.1 Develop security policies] The organisation shall develop high-level cyber security policies for the industrial automation and control system environment which are approved by management.

ID	SM 1.2
Measure	Organisation of information security.
Definition	The provider should establish and maintain an appropriate structure of security roles and responsibilities.
Example	[From IEC 62443 - 4.3.2.3.2 Establish the security organization(s)] There shall be an organisation, structure or network of stakeholders established (or chosen) under management leadership, with the responsibility to provide clear direction and oversight for the cyber aspects of the industrial automation and control system. [From NERC CIP-003-4 - Requirement 2 Leadership] The responsible entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards.

ID	SM 1.3
Measure	Information security procedures.
Definition	The provider should establish and maintain an appropriate set of security procedures that supports the implementation of the security policy.
Example	[From IEC 62443 - 4.3.2.6.2 Develop security procedures] The organisation shall develop and approve cyber security procedures, based on the cyber security policies and provide guidance in how to meet the policies. [From NISTIR 7628 - SG.PM-1 Security Policy and Procedures -Requirement 1.b[5]] The organisation develops, implements, reviews, and updates on an organisation-defined frequency procedures to address the implementation of the security program security policy and associated security program protection requirements.

ID	SM 1.4
Measure	Risk management framework.
Definition	The provider should establish and maintain an appropriate risk management framework for risk assessment and risk treatment activities across the organisation which will take into account the complex operational environment.
Example	[From NISTIR 7628 - SG.PM-5 Risk Management Strategy - Requirements 1 and 2] The organisation develops, a comprehensive strategy to manage risk to organisational operations and assets, individuals, and other organisations associated with the operation and use of information systems; and implements that strategy consistently across the organisation. [From IEC 62443 - 4.2.3.1 Select a risk assessment methodology] The organisation shall select a particular risk assessment and analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their industrial automation and control system assets.

ID	SM 1.5
Measure	Risk assessment.
Definition	The provider should establish and perform risk assessment activities to identify and evaluate the risk across the organisation at regular intervals.
Example	[From ISO/IEC 27002 - 4.1 Assessing security risks] Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organisation. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing

[5] *The material quoted is only part of a requirement in the original text. For instance, in SM1.3, the material quoted is only one of a seven-part requirement (SG.PM-1 Requirement 1.b).*

	controls selected to protect against these risks. [From ISO/IEC TR 27019 - 4.2.4.1.a Establishment of information security management] Through risk assessment, threats to the organisation's own assets will be identified; vulnerabilities and likelihood of occurrence will be evaluated and potential impact assessed.

ID	SM 1.6
Measure	Risk treatment plan.
Definition	The provider should establish and maintain an appropriate risk treatment plan in order to manage the risk across the organisation.
Example	[From NISTIR 7628 - SG.RA-2 Risk Management Plan - Supplemental Guidance[6]] Risk mitigation measures need to be implemented and the results monitored against planned metrics to ensure the effectiveness of the risk management plan. [From IEC 62443 - 4.3.4.2.2 Employ a common set of countermeasures] A common defined set of countermeasures (technical and administrative) to address both physical and cyber security risks should be defined and applied across the organisation wherever a specific risk is identified.

3.2 Domain 2: 2. Management of third parties

Control Objective: The provider has established and maintained a third parties management program that involves agreements on security related issues with the smart grid's stakeholders that participate in the smart grid value chain. These agreements should also take account of the supply chain as appropriate.

ID	SM 2.1
Measure	Third party agreements.
Definition	The provider should establish and maintains appropriate third party agreements to preserve the integrity, confidentiality and availability of the information at the same level as the internal services when dealing with customers and third parties.
Example	[From NISTIR 7628 - SG.SA-2 Security Policies for Contractors and Third Parties - Requirement 1] External suppliers and contractors that have an impact on the security of smart grid information systems must meet the organisation's policy and procedures. [From ISO/IEC 27036 – Part 2 - 6.1.1 Acquisition process - Objective] The following objective shall be met by the acquirer for successfully managing information security

[6] *Supplemental guidance provides additional information that may be useful in understanding the security requirement.*

	within the acquisition process: Establish a supplier relationship strategy that: • Is based on the information security risk tolerance of the acquirer; • Defines the information security foundation to use when planning, preparing, managing and terminating the procurement of a product or service. [From ISO/IEC 27002 - 6.2.1 Identification of risks related to external parties] The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

ID	SM 2.2
Measure	Monitoring third parties services and validating solutions against predefined acceptance criteria.
Definition	The provider should establish and maintain mechanisms in order to monitor the compliance of contractual obligations of information and services and validate solutions against predefined acceptance criteria.
Example	[From ISO/IEC 27002 - 10.2 Third party service delivery management] The organisation should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party. [From NISTIR 7628 - SG.AU-1 Audit and Accountability Policy and Procedures - Requirement 1.a.ii.] The scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties.

3.3 Domain 3: Secure lifecycle process for smart grid components/systems and operating procedures

Control Objective: The provider has established and maintained a secure lifecycle process that involves the planning, requirements definition, development, deployment, configuration, operation and disposal of the smart grid components/systems and procedures.

Security measures applicable to smart grid **components/systems** are:

ID	SM 3.1
Measure	Security requirements analysis and specification[7].
Definition	The provider should identify and define beforehand the necessary security requirements

[7] *These security requirements should be aligned with the M/490 SG-CG/SGIS Working Group recommendations.*

	for smart grid components and systems during the design and procurement.
Example	[From ISO/IEC 27002 - 12.1.1 Security requirements analysis and specification] Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. [From NISTIR 7628 - SG.SA-8 Security Engineering Principles – General Requirement] The organization applies security engineering principles in the specification, design, development, and implementation of any Smart Grid information system.

Security measures applicable to smart grids **operating procedures** are:

ID	**SM 3.2**
Measure	Inventory of smart grid components/systems.
Definition	The provider should establish and maintain an inventory that represents the components and smart grid information systems.
Example	[From ISO/IEC 27002 - 7.1.1 Inventory of assets] All assets should be clearly identified and an inventory of all important assets drawn up and maintained. [From NISTIR 7628 - SG.CM-8 Component Inventory - Requirement 1] The organisation develops, documents, and maintains an inventory of the components of the smart grid information system that accurately reflects the current Smart Grid information system configuration. [From NERC CIP-002-4a Requirement 1 - Critical Asset Identification] The Responsible Entity shall develop a list of its identified critical assets determined through an annual application of the criteria contained in the NERC CIP Standard.

ID	**SM 3.3**
Measure	Secure configuration management of smart grid components/systems.
Definition	The provider should ensure that the base security configuration of a smart grid's components/systems is identified, set and maintained for every instance of that component/system.
Example	[From NISTIR 7628 - SG.CM-10 Factory Default Settings Management - Requirement 1] The organisation policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on smart grid information system components and applications. [From ISO/IEC TR 27019 - B.1.1.1.9 Secure Standard Configuration, Installation and Start-Up] After initial installation and start-up the system should be configured in a fail-safe and secure manner. The defined secure base configuration should be documented.

ID	SM 3.4
Measure	Maintenance of smart grid components/systems.
Definition	The provider should establish and maintain activities for performing routine and preventive/corrective maintenance on the components and smart grid information systems.
Example	[From NISTIR 7628 - SG.MA-3 Smart Grid Information System Maintenance - Requirement 1] The organisation schedules, performs, documents, and reviews records of maintenance and repairs on smart grid information system components in accordance with manufacturer or vendor specifications and/or organisational requirements. [From ISO/IEC 27002 - 9.2.4 Equipment maintenance] Equipment shall be correctly maintained to ensure its continued availability and integrity.

ID	SM 3.5
Measure	Software/firmware upgrade of smart grid components/systems.
Definition	The provider should establish and maintain activities for software/firmware upgrade on the components and smart grid information systems.
Example	[From NISTIR 7628 - SG.SI-2 Flaw Remediation - Requirement 1 and 2] The organisation identifies, reports, and corrects Smart Grid information system flaws and tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation. [From ISO/IEC 27002 - 12.5.3 Restrictions on changes to software packages] A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software.

ID	SM 3.6
Measure	Disposal of smart grid components/systems.
Definition	The provider should establish and maintain activities for the secure disposal of smart grid components and smart grid information systems.
Example	[From NISTIR 7628 - SG.CM.9 - Addition, Removal, and Disposal of Equipment – Requirement 1] The organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment. [NERC CIP-007-4 - Requirement 7. Disposal or Redeployment] The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in NERC CIP standard.

Security measures applicable to smart grids **components/systems and procedures** are:

ID	SM 3.7
Measure	Security testing of smart grid components/systems.[8]
Definition	Security testing activities on the smart grid components/systems should be performed in order to verify its security.
Example	[From NISTIR 7628 - SG.SI-6 Security Functionality Verification - Requirement 1.a] The organisation verifies the correct operation of security functions within the smart grid information system Smart Grid information system start up and restart. [From IEC 62443 - 4.3.4.3.1 Define and test security functions and capabilities] The security functions and capabilities of each new component of the industrial automation and control system assets shall be defined up front, developed or achieved via procurement, and tested together with other components so that the entire system meets the desired security profile.

3.4 Domain 4: Personnel security, awareness and training

Control Objective: **The provider has established and maintained a personnel security, awareness and training program that supports a culture of cyber security for all relevant stakeholders and fosters the mutual exchange of security information between electric sector and information security professionals in the smart grid value chain.**

ID	SM 4.1
Measure	Personnel screening.
Definition	The provider should perform appropriate background checks on personnel (employees, contractors, and third-party users) if required for their duties and responsibilities.
Example	[From NERC CIP-004-3a - Requirement 3 Personnel Risk Assessment] The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. [From ISO/IEC TR 27019 - 8.1.2 Screening] A strict screening process for key personnel

[8] *It is recognized that it is important and desirable to additionally provide appropriate security certification for components and/or systems. However, given the lack of appropriate certification schemes and the current maturity level of the existing ones, it is currently not possible to generally require certification on a European scale. Further work needs to be facilitated to reach a multi-stakeholder, European wide approach for identifying security risks in order to be able to derive appropriate requirements. This contributes to ensure a commonly accepted certification scheme on European level for products. It is recommended to increase and accelerate efforts towards a European certification strategy to enable such a requirement.*

	that have access to critical information assets or that are responsible for the operation and maintenance processes of critical systems should be considered. This is especially the case if the information assets or systems are part of the critical infrastructure or if they are required for the operation of critical infrastructure.

ID	SM 4.2
Measure	Personnel changes.
Definition	The provider should establish and maintain an appropriate process for managing changes in personnel (employees, contractors, third-party users) or changes in their roles and responsibilities.
Example	[From NISTIR 7628 - SG.PS-5 Personnel Transfer - Requirement 1] The organization reviews logical and physical access permissions to smart grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. [From ISO/IEC 27002 - 8.3 Termination or change of employment] Responsibilities should be in place to ensure an employee's, contractors or third-party user's exit from the organisation is managed, and that the return of all equipment and the removal of all access rights are completed.

ID	SM 4.3
Measure	Security and awareness program.
Definition	The provider should establish and maintain a security awareness program across the organisation.
Example	[From NISTIR 7628 - SG.AT-1 Awareness and Training Policy and Procedures - Requirement 1.a] The organization develops, implements, reviews, and updates on an organization-defined frequency a documented awareness and training security policy that addresses: • The objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets, and • The scope of the awareness and training security program as it applies to all of the organizational staff, contractors, and third parties. [From IEC 62443 - 4.3.2.4.1 Develop a training program] The organisation shall design and implement a cyber-security training program. [From ISO/IEC 27002 - 8.2.2 Information security awareness, education, and training] All employees of the organisation and, where relevant, contractors and third-party users should receive appropriate awareness training. [From NISTIR 7628 – SG.AT-2 Security Awareness - General Requirement] The organisation provides basic security awareness briefings to all smart grid information

	system users (including employees, contractors, and third parties) on an organisation-defined frequency.

ID	SM 4.4
Measure	Security training and certification of personnel.
Definition	The provider should establish and maintain security training and personnel certification programmes, taking into account its needs based on their roles and responsibilities.
Example	[From NISTIR 7628 – SG.AT-3 Security Training - Requirement 1] The organisation provides security-related training before authorizing access to the smart grid information system or performing assigned duties. [From IEC 62443 - 4.3.2.4.3 Provide training for support personnel] All personnel that perform risk management, industrial automation and control system engineering, system administration/maintenance and other tasks that impact the cyber security management system should be trained on the security objectives and industrial operations for these tasks.

3.5 Domain 5: Incident response & information knowledge sharing

Control Objective: The provider has established and maintained an incident response and information knowledge sharing process that prevents, resolves and recovers from cyber events, effectively containing the damage, and allows sharing cyber security information for internal and external entities.

ID	SM 5.1
Measure	Incident response capabilities.
Definition	The provider should establish and maintain capabilities to respond against cyber security incidents.
Example	[From NISTIR 7628 - SG.IR-1 Incident Response Policy and Procedures - Requirement 1.a] The organization develops, implements, reviews, and updates on an organization-defined frequency a documented incident response security policy that address: • The objectives, roles, and responsibilities for incident response security program as it relates to protecting the organization's personnel and assets, and; • The scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties. [From IEC 62443 - 4.3.4.5.1 Implement an incident response plan] The organisation shall implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals.

ID	SM 5.2
Measure	Vulnerability assessment.
Definition	The provider should establish and maintain vulnerability assessment activities on the smart grid information systems.
Example	[From NISTIR 7628 - SG.RA-6 Vulnerability Assessment and Awareness - Requirement 1] The organisation monitors and evaluates the smart grid information system according to the risk management plan on an organisation-defined frequency to identify vulnerabilities that might affect the security of a smart grid information system. [From IEC 62443 - 4.2.3.7 Perform a detailed vulnerability assessment] The organization shall perform a detailed vulnerability assessment of its individual logical industrial automation and control system, which may be scoped based on the high-level risk assessment results and prioritization of industrial automation and control system subject to these risks.

ID	SM 5.3
Measure	Vulnerability management.
Definition	The provider should establish and maintain an appropriate vulnerability management plan in order to manage vulnerabilities on smart grid information systems.
Example	[From ISO/IEC 27002 - 12.6.1 Control of technical vulnerabilities] Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities. [From IEC 62443 - 4.2.3.14 Maintain vulnerability assessment records] Up-to-date vulnerability assessment records should be maintained for all assets comprising the industrial automation and control system.

ID	SM 5.4
Measure	Contact with authorities and security interest groups.
Definition	The provider should establish and maintain contacts with authorities and security interest groups to be aware of vulnerabilities and threats.
Example	[From ISO/IEC TR 27019 - 6.1.6 Contact with authorities] The applications and infrastructure of energy utility process control systems may be considered as part of the critical infrastructure and may be essential for the functioning of the local community and society and the economy as a whole. Operators of such systems should therefore maintain contact with all of the relevant authorities. [From ISO/IEC 27002 - 6.1.6 Contact with authorities] Appropriate contacts with relevant authorities should be maintained.

3.6 Domain 6: Audit and accountability

Control Objective: The provider has established and maintained an audit and accountability process that enables sufficient logging capabilities in the smart grid systems and components and provides valuable log data for analysis.

ID	SM 6.1
Measure	Auditing capabilities.
Definition	The provider should establish and maintain auditing capabilities on the smart grid Information systems and components.
Example	[From NISTIR 7628 - SG.AU-15 Audit Generation - Requirement 1] The smart grid information system provides audit record generation capability and generates audit records for the selected list of auditable events. [From ISO/IEC TR 27019 - 10.10.1 Audit logging] Relevant audit events may also include certain actions carried out by operating personnel, such as switching operations for instance.

ID	SM 6.2
Measure	Monitoring of smart grid information systems.
Definition	The provider should establish and maintain monitoring activities on the smart grid Information systems and components.
Example	[From NERC CIP-005-4a - Requirement 3. Monitoring Electronic Access] The Responsible Entity should implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week. [From ISO/IEC 27002 - 10.10 Monitoring] Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.

ID	SM 6.3
Measure	Protection of audit information.
Definition	The provider should protect the audit information generated.
Example	[From ISO/IEC 27002 - 10.10.3 Protection of log information] Logging facilities and log information should be protected against tampering and unauthorized access. [From NISTIR 7628 - SG.AU-9 Protection of Audit Information - General Requirement] The smart grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.

3.7 Domain 7: Continuity of operations

Control Objective: The provider has established and maintains a continuity of operations process that allows continuing or resuming operations of a smart grid information system in the event of disruption of normal system operation.

ID	SM 7.1
Measure	Continuity of operations capabilities[9].
Definition	The provider should establish and maintain capabilities to ensure essential functions after disruption events on smart grid Information systems.
Example	[From NISTIR 7628 - SG.CP-2 Continuity of Operations Plan - Requirement 1] The organisation develops and implements a continuity of operations plan dealing with the overall issue of maintaining or re-establishing operations in case of an undesirable interruption for a smart grid information system. [From ISO/IEC TR 27019 - 14.1.1 Including information security in the business continuity management process] Energy utility organisations should consider the continuity of the general energy supply as one of the key elements of business continuity management.

ID	SM 7.2
Measure	Essential communication services.
Definition	The provider should establish, maintain and test essential/emergency communication services in case of major disasters.
Example	[From NISTIR 7628 - SG.CP-11 Fail-Safe Response - General Requirement] The smart grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart grid information systems or the loss of the smart grid information system itself. [From ISO/IEC TR 27019 - 14.2.1 Emergency communication] Energy utility organisations should ensure that essential communication links are maintained with their own emergency staff and/or the emergency staff of other utilities, with essential control systems and with external emergency organisations necessary for the protection and handling of, or recovery from such incidents.

[9] *It is important to highlight the fact that the design of the smart grid architecture need to be done taking into account the requirements that will allow the implementation of a resilient infrastructure against cyber-attacks.*

3.8 Domain 8: Physical security

Control Objective: The provider has established and maintained a physical security program that restricts the access to smart grid information systems and components only to authorized personnel.

ID	SM 8.1
Measure	Physical security.
Definition	The provider should establish and maintain the appropriate physical security of the smart grid facilities/components/systems.
Example	[From ISO/IEC 27002 - 9.1 Secure areas] Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorised access, damage, and interference. The protection provided should be commensurate with the identified risks. [From NISTIR 7628 - SG.PE-3 Physical Access - Requirement 1] The organisation enforces physical access authorizations for all physical access points to the facility where the smart grid information system resides.

ID	SM 8.2
Measure	Logging and monitoring physical access.
Definition	The provider should establish and maintain capabilities for logging and monitoring the physical access to the smart grid facilities/components taking into account the criticality of the facility.
Example	[From NERC CIP-006 - Requirement 4. Physical Access Controls] The Responsible Entity should document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. [From IEC 62443 - 4.3.3.3.8 Establish procedures for monitoring and alarming] Procedures should be established for monitoring and alarming when physical or environmental security is compromised.

ID	SM 8.3
Measure	Physical security on third party premises.
Definition	The provider should protect equipment located outside of the organisations' own grounds or premises in areas that are the responsibility of other utilities against physical and environmental threats.
Example	[From ISO/IEC TR 27019 - 9.3.1 Equipment sited on the premises of other energy utility organizations] Where energy utility organisations install equipment outside of their own

	grounds or premises in areas that are the responsibility of other utilities, such as transfer stations for instance, the equipment should be sited in a protected area so that any risks arising from environmental threats or dangers are mitigated and the possibility of unauthorized access is reduced. [From ISO/IEC 27002 -9.2.5 Security of equipment off premises] Security shall be applied to off-site equipment taking into account the different risks of working outside the organisation's premises.

3.9 Domain 9: Information systems security

Control Objective: The provider has established and maintained information systems security controls that ensure that the smart grid information systems and components are logically accessed only by authorized entities and that its information is properly protected[10].

ID	SM 9.1
Measure	Data security.
Definition	The provider should implement security requirements in order to protect the information on smart grid information system.
Example	[From ISO/IEC TR 27019 - B.1.1.1.6 Encryption of Sensitive Data during Storage and Transmission] Sensitive data should be stored or transmitted in encrypted form only. [From ISO/IEC 27002 - 10.7.3 Information handling procedures] Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

ID	SM 9.2
Measure	Account management.
Definition	The provider should establish and maintain system/groups/user accounts on smart grid information systems.
Example	[From ISO/IEC 27002 - 11.2 User access management] The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls. [From NISTIR 7628 - SG.AC-3 Account Management - Requirement 1] The organisation

[10] *It is important to differentiate between data security (security of raw unprocessed information) and information security (security of the data that has been processed and it is valuable for the organisation).*

	manages smart grid information system accounts, including authorizing, establishing, activating, modifying, disabling, and removing accounts.

ID	SM 9.3
Measure	Logical access control.
Definition	The provider should enforce logical access to authorized entities on smart grid information systems and security perimeters.
Example	[From NERC CIP-003-4 - Requirement 5. Access Control] The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information. [From IEC 62443 - 4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices] The permission to access industrial automation and control system devices shall be logical (rules that grant or deny access to known users based on their roles).

ID	SM 9.4
Measure	Secure remote access.
Definition	The provider should establish and maintain secure remote access where applicable to smart grid information systems.
Example	[From NISTIR 7628 - SG.AC-2 Remote Access Policy and Procedures - Requirement 1] The organisation documents allowed methods of remote access to the smart grid information system. [From IEC 62443 - 4.3.3.6.6 Develop a policy for remote login and connections] The organisation shall develop a policy addressing remote login by a user and/or remote connections (for example, task-to-task connections) to the control system which defines appropriate system responses to failed login attempts and periods of inactivity.

ID	SM 9.5
Measure	Information security on information systems.
Definition	The provider should establish and maintain appropriate information security capabilities on information systems, to provide protection against malware, viruses and other common threats.
Example	[From IEC 62443 - 4.3.4.3.8 Establish and document antivirus/malware management procedure] A procedure for antivirus/malware management shall be established, documented, and followed. [From ISO/IEC TR 27019 - 10.4.1 Controls against malicious code] The possible effects of malware incidents on equipment used for real-time process control and associated

	communications (e.g. through overload and disruption) should be taken into consideration and mitigated by implementing the appropriate controls.

ID	SM 9.6
Measure	Media handling.
Definition	The provider should establish and maintain secure procedures for the access, storage, distribution, transport, sanitization, destruction and disposal of the media assets.
Example	[From NISTIR 7628 - SG.MP-1 Media Protection Policy and Procedures – Requirement 1a] The organization develops, implements, reviews, and updates on an organization-defined frequency a documented media protection security policy that addresses: i. The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets, and; ii. The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties. [From ISO/IEC 27002 - 10.7.1 Management of removable media] There should be procedures in place for the management of removable media.

3.10 Domain 10: Network security

Control Objective: The provider has established and maintains a secure network engineering program that prevents security controls from being circumvented.

ID	SM 10.1
Measure	Secure network segregation.
Definition	The provider should establish and maintain a segregated network for the smart grid information system.
Example	[From ISO/IEC 27002 - 11.4.5 Segregation in networks] Groups of information services, users, and information systems should be segregated on networks. [From ISO/IEC TR 27019 - 11.4.5 Segregation in networks] Where applicable and technically feasible, the network infrastructure of process control systems should be divided into multiple zones with different functions and protection requirements. In particular, different technical and operational domains should be segregated from one another.

ID	SM 10.2
Measure	Secure network communications.
Definition	The provider should establish and maintain secure communications across the segregated network.
Example	[From NISTIR 7628 - SG.SC-9 Communication Confidentiality - General Requirement] The smart grid information system protects the confidentiality of communicated information. [From ISO/IEC 27011 – A.10.6 Network security management] The secure management of networks, which may span organizational boundaries, requires careful consideration to data flow, legal implications, monitoring, and protection. [From ISO/IEC 27002 - 11.4.7 Network routing control] Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

4 Sophistication levels

This section presents the sophistication levels that apply to the defined smart grids security measures for each of the 10 domains previously identified.

4.1 Domain 1: Security governance & risk management

Control Objective:
The provider has established and maintains a security governance program that directs and controls the smart grid information security. It provides strategic direction, ensures objectives are achieved, cyber security risk aspects regarding the smart grid systems and components have been fully addressed, uses organisational resources responsibly, and monitors the success or failure of the security programme. It should be noted that the programme should identify not only the internal risks but also risks coming from ICT and energy supply chain as appropriate.

SM 1.1 Information security policy.
The provider should establish and maintain an appropriate information security policy.

Level	Practices	Evidence
1	✓ Minimum security activities on the smart grid information system are performed by the organisation.	✓ Documented security procedures that address the minimum security activities.
2	✓ An information security policy that addresses a secure and reliable energy supply and legal and regulatory requirements is available and approved by management. ✓ Employees are aware of the existence and behave accordingly.	✓ Approved information security policy covering most aspects of security containing at least: ○ Scope of the information security policy; ○ Applicable laws and regulations; ○ Security objectives; ○ Management commitment with the security policy. ✓ Proof of the information security policy communication among staff. ✓ The information security policy is easy accessible for staff.
3	✓ The information security policy is regularly reviewed[11] at planned intervals or	✓ Last planned review has been done according with the review process.

[11] *The interval depends on the specifics of the organisation.*

SM 1.1 Information security policy. The provider should establish and maintain an appropriate information security policy.		
Level	**Practices**	**Evidence**
	if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	✓ Records of the management review. ✓ Meeting minutes of review sessions.

SM 1.2 Organisation of information security. The provider should establish and maintain an appropriate structure of security roles and responsibilities.		
Level	**Practices**	**Evidence**
1	✓ Security roles and responsibilities are defined in the organisation.	✓ Chart that reflects the organisation of information security.
2	✓ Security roles and responsibilities are established and documented separating functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles. ✓ Security roles and responsibilities are assigned to staff that is adequately positioned within the organisation, taking into account the specific, size, and necessities of the department and qualifications of the person.	✓ The organisation of information security is adequately positioned within the organisation. ✓ Formal description of the key security roles and responsibilities. ✓ Formal appointment of the key security roles and responsibilities.
3	✓ A backup person has been designated for key security roles and responsibilities.	✓ Formal appointment of the backup person.

SM 1.3 Information security procedures. The provider should establish and maintain an appropriate set of security procedures that supports the implementation of the security policy.		
Level	**Practices**	**Evidence**
1	✓ Security procedures to address the key security activities are developed, implemented and documented.	✓ Formal description of the key security procedures containing at least: ○ Objectives, roles, and responsibilities; ○ Scope of the security procedure; ○ Security objectives.
2	✓ Security procedures to address the information security policy are developed, implemented and documented.	✓ Formal description of the security procedures containing at least: ○ Objectives, roles, and responsibilities;

SM 1.3 Information security procedures. The provider should establish and maintain an appropriate set of security procedures that supports the implementation of the security policy.		
Level	**Practices**	**Evidence**
		○ Scope of the security procedure; ○ Security objectives.
3	✓ Security procedures that address the information security policy are reviewed and updated on a regular basis.	✓ The last planned review has been done according with the review process. ✓ Meeting minutes of review sessions.

SM 1.4 Risk management framework. The provider should establish and maintain an appropriate risk management framework for risk assessment and risk treatment activities across the organisation which will take into account the complex operational environment.		
Level	**Practices**	**Evidence**
1	✓ The risk management methodology has been developed based on best practices and standards related to the information and communications technology context.	✓ Documented risk management methodology that covers the risk on information and communication technology containing at least: ○ Objectives, roles, and responsibilities; ○ Scope of the risk management methodology; ○ Procedures that supports the risk assessment. ✓ Formal description of the risk tolerance level. ✓ Organisation inventory assets that includes facilities, personnel, premises, etc.
2	✓ The risk management methodology has been developed based on best practices and standards related to the smart grid information system context.	✓ Documented risk management methodology that covers the risk on smart grids information system containing at least: ○ Objectives, roles, and responsibilities; ○ Scope of the risk management methodology; ○ Procedures that supports the risk assessment; ○ Catastrophic but improbable events that could affect to the smart grids. ✓ Formal description of the risk tolerance level.
3	✓ The risk management methodology is updated on a regular basis to ensure its	✓ The last planned review has been done according with the review process.

SM 1.4 Risk management framework. The provider should establish and maintain an appropriate risk management framework for risk assessment and risk treatment activities across the organisation which will take into account the complex operational environment.		
Level	**Practices**	**Evidence**
	continuing suitability, adequacy, and effectiveness.	✓ Meeting minutes of review sessions.

SM 1.5 Risk assessment. The provider should establish and perform risk assessment activities to identify and evaluate the risk across the organisation at regular intervals.		
Level	**Practices**	**Evidence**
1	✓ Risk assessment activities are executed following the defined methodology.	✓ Documented risk assessment activities results containing at least: ○ Critical assets identification; ○ Vulnerabilities; ○ Threat sources; ○ Security impact level; ○ Organisation risk level.
2	✓ Risk assessment activities take into consideration the risk resulting from third party access (e.g. vendors, system integrators or business partners) to sensitive systems, networks and information.	✓ Documented risk assessment activities results containing at least: ○ The risk on process control systems where system vendors and integrators are involved in the maintenance and operation processes of these systems; ○ The risk on the use of remote access connections for maintenance by external parties; ○ The risk on the access to security-controlled areas to perform on-site maintenance by external parties; ○ The risk on coupling of the control systems and communication networks of different organizations.
3	✓ Risk assessment activities are executed on a regular basis or whenever significant changes occur to the smart grid information system.	✓ The last planned review has been done according with the review process. ✓ Meeting minutes of review sessions.

SM 1.6 Risk treatment plan. The provider should establish and maintain an appropriate risk treatment plan in order to manage the risk across the organisation.		
Level	**Practices**	**Evidence**
1	✓ A risk treatment plan is developed based on the results of the risk assessment activities.	✓ Documented risk treatment plan containing at least: ○ Risk identified; ○ Risk treatment; ○ Security measure to implement.
2	✓ The risk treatment plan is reviewed and approved by the management.	✓ Records of the management review. ✓ Management commitment with the treatment plan.
3	✓ The effectiveness of the measures proposed on the risk treatment plan is reviewed on a regular basis.	✓ The last planned review has been done according with the review process. ✓ Meeting minutes of review sessions.

4.2 Domain 2: Management of third parties

Control Objective:
The provider has established and maintains a third parties management program that involves agreements on security related issues with the smart grid's stakeholders that participate in the smart grid value chain. These agreements should also take account of the supply chain as appropriate.

SM 2.1 Third party agreements. The provider should establish and maintain appropriate third party agreements to preserve the integrity, confidentiality and availability of the information at the same level as the internal services when dealing with customers and third parties.		
Level	**Practices**	**Evidence**
1	✓ Contractual agreements when dealing with third parties and customers have been established. ✓ Security measures to protect the customer access to information have been defined (see domain 9 Information systems security). ✓ Responsibilities regarding the maintenance, operation and ownership of	✓ List of relevant third party relationships. ✓ List of customer access request. ✓ Identify selection criteria. ✓ Documented contractual agreements containing at least: ○ Service description;

SM 2.1 Third party agreements. The provider should establish and maintain appropriate third party agreements to preserve the integrity, confidentiality and availability of the information at the same level as the internal services when dealing with customers and third parties.		
Level	**Practices**	**Evidence**
	assets have been defined.	○ Security measures; ○ Non-disclosure agreements; ○ Roles and responsibilities; ○ Target service levels; ○ Contacts and reporting lines.
2	✓ Special requirements relating to crisis and emergency communication where telecommunication services for the process control systems are supplied by third parties have been identified. ✓ Preventive measures that may need to be taken in case of service overload and to ensuring an acceptable degree of independence of the telecommunication services of external energy utilities have been identified.	✓ Documented third parties contractual agreements contains special requirements in case of: ○ Major blackouts; ○ Natural catastrophes; ○ Accidents or other possible emergency situations; ○ Blackout resistance.
3	N/A	N/A

SM 2.2 Monitoring third parties services and validating solutions against predefined acceptance criteria. The provider should establish and maintain mechanisms in order to monitor the compliance of contractual obligations of information and services and validate solutions against predefined acceptance criteria.		
Level	**Practices**	**Evidence**
1	✓ Security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	✓ Documented service level agreement that contains requirement to protect confidentiality, integrity and availability of information.
2	✓ Services provided by the third party are monitored and reviewed on a regular basis. ✓ Regularly auditing activities are implemented on the third party. ✓ Changes to the provision of services, are managed taking into account the criticality of business systems and processes involved and re-assessment of risk aspects.	✓ Documented results of monitoring activities. ✓ Documented results of auditing activities. ✓ Identify the process(es) applied to manage recent changes and confirm: ○ Adequate warning is provided; ○ Involves relevant personnel; ○ Includes procedures for backing-out from failed changes.

SM 2.2 Monitoring third parties services and validating solutions against predefined acceptance criteria. The provider should establish and maintain mechanisms in order to monitor the compliance of contractual obligations of information and services and validate solutions against predefined acceptance criteria.		
Level	**Practices**	**Evidence**
3	N/A	N/A

4.3 Domain 3: Secure lifecycle process for smart grid components/systems and operating procedures

Control Objective:
The provider has established and maintained a secure lifecycle process that involves the planning, requirements definition, development, deployment, configuration, operation and disposal of the smart grid components/systems and procedures.

SM 3.1 Security requirements analysis and specification. The provider should identify and define beforehand the necessary security requirements for smart grid components and systems during the design and procurement.		
Level	**Practices**	**Evidence**
1	✓ Security requirements for security are specified early stages of information during the design and procurement of smart grid components and systems. ✓ Security requirements take into account the electromagnetic emanations of the smart grid information systems and components. ✓ Secure coding practices are used to reduce common security errors.	✓ Documented security requirements. ✓ Documented secured coding practices and guidelines.
2	✓ A threat model is created for each smart grid information system and component. ✓ Security requirements are updated based on the results of the threat model.	✓ Documented threat model. ✓ Updated documented security requirements based on the threat plan output.
3	✓ A documented and tested security response plan is created in the event vulnerability is discovered. ✓ Root cause analysis is performed in order to understand the cause of identified vulnerabilities.	✓ Documented security response plan. ✓ Documented analysis of identified vulnerabilities.

SM 3.2 Inventory of smart grid components/systems. The provider should establish and maintain an inventory that represents the components and smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ An inventory of assets of the smart grid components and information systems is available and maintained in the organisation. ✓ The responsibilities in relation to smart grid components and information systems and the roles of the asset owner and asset operator in respect of information security are exactly defined and documented.	✓ Documented inventory of assets containing at least: ○ Relevant process control systems; ○ Information assets; ○ Application; ○ Physical assets; ○ Services; ○ Operating system/firmware; ○ Legacy systems; ○ Location (logical and physical) of each component; ○ Owners; ○ Roles and responsibilities. ✓ The last planned review has been done according with the review process. ✓ Meeting minutes of review sessions.
2	✓ Rules for the acceptable use of smart grid components and information systems are identified, documented and implemented. ✓ The implemented multiple zones with different functions and protection requirements defined on the network infrastructure are included as a part of the inventory. ✓ The implemented independent horizontal segments defined on networks and distributed systems are included as a part of the inventory. ✓ The implemented specific network for patch management functions defined on networks is included as a part of the inventory.	✓ Documented acceptable use of smart grid components. ✓ Documented inventory of assets containing the defined zones and segments.
3	✓ Smart grid components and information systems are classified in terms of value, legal requirements, sensitivity and criticality to the organisation. ✓ An appropriate set of procedures for information labelling and handling should be developed and implemented in accordance with the classification scheme adopted by the organisation.	✓ Documented classification schema covering at least the following smart grid components and systems: ○ Corporate assets, systems and information supporting the operation of critical infrastructures and sensitive systems; ○ Corporate assets, systems and information needed for restoration of the energy supply system following a major supply disruption (grid

SM 3.2 Inventory of smart grid components/systems. The provider should establish and maintain an inventory that represents the components and smart grid information systems.		
Level	**Practices**	**Evidence**
		restoration); ○ Corporate assets, systems and information necessary to ensure functional safety/plant security; ○ Corporate assets, systems and information necessary to ensure functional safety, to fulfil regulatory requirements such as unbundling requirements for instance, or that need to be implemented in order to fulfil other specific requirements. ✓ Identify labelling/handling procedures for the classification schema defined.

SM 3.3 Secure configuration management of smart grid components/systems. The provider should ensure that the base security configuration of a smart grid's components/systems is identified, set and maintained for every instance of that component/system.		
Level	**Practices**	**Evidence**
1	✓ A secure baseline configuration of smart grid components and information systems is developed, documented and maintained. ✓ Configuration changes are tested, validated and documented before installing on the operational smart grid information system. ✓ Only authorized individuals are allowed to obtain access to smart grid components and information systems for purposes of initiating changes, including upgrades, and modifications.	✓ Documented secure baseline configuration containing at least: ○ Essential capabilities of operation; ○ Restricted use of functions; ○ Ports, protocols and/or services allowed. ✓ Documented change management responsibilities and procedures. ✓ Documented and approved change control records.
2	✓ Periodical reviews of smart grid components and information systems in order to ensure compliance with established secure configuration baseline and applicable laws and regulations are performed. ✓ Exceptions to the configuration baseline are identified, documented and approved.	✓ Documented results of the compliance activities. ✓ Documented and approved exceptions to the configuration baseline containing the alternative controls in place to ensure the confidentiality, availability and integrity of the smart grid component.
3	✓ A secure baseline configuration for development and test environments is managed separately from the operational baseline configuration.	✓ Documented secure baseline configuration for development and test environments.

SM 3.3 Secure configuration management of smart grid components/systems. The provider should ensure that the base security configuration of a smart grid's components/systems is identified, set and maintained for every instance of that component/system.		
Level	**Practices**	**Evidence**
	✓ Automated mechanisms are implemented to centrally manage, apply, and verify configuration settings. ✓ Automated mechanisms enforce access restrictions and support auditing of the enforcement actions.	✓ Documented results of the execution of the automated tools.

SM 3.4 Maintenance of smart grid components/systems. The provider should establish and maintain activities for performing routine and preventive/corrective maintenance on the components and smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ Maintenance on smart grid information components is done in accordance with manufacturer or vendor specifications and/or organizational requirements. ✓ A list of qualified personnel authorized to perform maintenance on the smart grid information system is elaborated, documented and available. ✓ Access to Information data is controlled during the maintenance activities.	✓ Proof maintenance and reparation operations. ✓ List of personnel authorized to perform maintenance.
2	✓ Maintenance activities are formally scheduled. ✓ Approved equipment is used on maintenance activities. ✓ Records of the maintenance operations are maintained. ✓ Remote maintenance activities are notified, authorized, planned and audited. ✓ Remote maintenance activities are performed by defined and trained contractor personnel using systems physically or logically disconnected from other systems and networks during a remote access session.	✓ List of planned maintenance actions. ✓ Formal authorization for remote maintenance activities and maintenance equipment. ✓ Approved documented security and evaluation plans containing at least: ○ Date and time; ○ Person who performs the activity; ○ Description of the activities performed; ○ List of equipment removed or replaced.
3	✓ Additional controls should be implemented when maintenance activities cannot be performed normally on smart grid information systems.	✓ Documented and approved exceptions to the maintenance process containing the alternative controls in place to ensure the availability and integrity of the smart grid information system and components.

SM 3.5 Software/firmware upgrade of smart grid components/systems. The provider should establish and maintain activities for software/firmware upgrade on the components and smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ Smart grid components affected by recently announced flaws are identified. ✓ Software/firmware updates are tested for effectiveness and potential side effects on organisational smart grid information systems and components before installation.	✓ Documented inventory of affected systems. ✓ Documented test results.
2	✓ Software/firmware updates are incorporated into the secure configuration management process (see measure SM 3.2 Secure configuration management of smart grid components). ✓ A single point of contact and communication channels for smart grid components security related issues with manufacturers or vendors have been identified.	✓ Evidences of the software/firmware inclusion into the secure configuration management process. ✓ List of manufactures single point of contact.
3	✓ Additional controls should be implemented when update activities cannot be performed normally on smart grid information systems.	✓ Documented and approved exceptions to the configuration baseline containing the alternative controls in place to ensure the confidentiality, availability and integrity of the smart grid component.

SM 3.6 Disposal of smart grid components/systems. The provider should establish and maintain activities for the secure disposal of smart grid components and smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ Smart grid information system and components are documented, identified, and tracked.	✓ Documented inventory of assets. ✓ Labelling of smart grid components.
2	✓ Smart grid information system components and information are checked to ensure that any sensitive data has been removed or securely overwritten prior to disposal or reuse. ✓ Smart grid information system components and information are taken-off with prior authorization. ✓ Disposal operations are performed by authorized personal.	✓ Formal authorization for disposal of Smart grid information system components and information. ✓ Documented results of secure wiping process. ✓ List of authorized personnel.

SM 3.6 Disposal of smart grid components/systems. The provider should establish and maintain activities for the secure disposal of smart grid components and smart grid information systems.		
Level	**Practices**	**Evidence**
3	✓ Alternative procedures for the secure remove of sensitive data are identified when normal procedures cannot be applied for technical reasons.	✓ Documented alternative procedures like secured destruction of the component.

SM 3.7 Security testing of smart grid components/systems. Security testing activities on the smart grid components/systems should be performed in order to verify its security.		
Level	**Practices**	**Evidence**
1	✓ Security functions and capabilities of new components are tested on non-operational environments individually and with other components in order to ensure the security of the entire system. ✓ Where applicable and technically feasible integrity checks of security-relevant settings and data at start-up are performed on a regular basis by the system or the security modules, respectively.	✓ Detailed security and stress test on the individual system components and on the entire system and its essential functions using a representative system configuration. ✓ Results of integrity checks or system fails.
2	✓ Approved and documented security test and evaluation plans are included as part of the lifecycle of the smart grid component. ✓ Static code and vulnerability analysis tools are used on a regular basis to test smart grid components[12]. ✓ Smart grid, SCADA systems and field devices are tested periodically to keep under control the risk level. ✓ End to end test are performed by the organisation in order to verify the security of smart grid components and information systems interconnected.	✓ Documented testing activities containing at least: ○ Objectives, roles, and responsibilities; ○ Scope of the plan; ○ Detailed results of the execution of the plan; ○ Frequency of the test. ✓ Results of automated tools. ✓ Results of end-to-end test.
3	✓ Additional security testing activities to determine the level of difficulty in circumventing the security requirements of the smart grid information	✓ Results of the additional security testing activities. ✓ Results of the smart grid component certification process.

[12] *The scope of the static code analysis depends on the type of the smart grid service provider. For instance, static code analysis can only be done by the vendor in its R&D environment.*

SM 3.7 Security testing of smart grid components/systems. Security testing activities on the smart grid components/systems should be performed in order to verify its security.		
Level	**Practices**	**Evidence**
	system have been defined. ✓ Recognised certification schemas are applied to smart grid components[13].	

4.4 Domain 4: Personnel security, awareness and training

Control Objective:
The provider has established and maintains a personnel security, awareness and training program that supports a culture of cyber security for all relevant stakeholders and fosters the mutual exchange of security information between electric sector and information security professionals in the smart grid value chain.

SM 4.1 Personnel screening. The provider should perform appropriate background checks on personnel (employees, contractors, and third-party users) if required for their duties and responsibilities.		
Level	**Practices**	**Evidence**
1	✓ Individuals screening criteria is established and reviewed for organisation's position. ✓ Individuals are screened before the access to the smart grid information systems is authorized.	✓ Screening records containing at least: ○ Employment history; ○ Verification of the highest education degree received; ○ Residency; ○ Law enforcement records.
2	✓ The screening process is in line with the defined policies and regulations. ✓ Individuals are rescreened based on a defined list of conditions.	✓ Documented screening requirements. ✓ Records of rescreening process.
3	✓ Specific security clearance provided by governmental organisations is required before the access to critical information assets.	✓ List of personnel who have access to critical information assets. ✓ List of personnel that hold a security clearance.

[13] *At the date of this study, there is no a recognized certification schema that can be generally applicable to smart grid components.*

SM 4.2 Personnel changes. The provider should establish and maintain an appropriate process for managing changes in personnel (employees, contractors, third-party users) or changes in their roles and responsibilities.		
Level	**Practices**	**Evidence**
1	✓ Responsibilities for performing employment termination or change of employment are clearly defined and assigned. ✓ Changes on personnel and operating arrangements are communicated to employees, customers, contractors or third parties. ✓ Logical and physical access to smart grid information systems are reconsidered based on the personnel changes. ✓ Organisation assets are returned upon termination of their employment, contract or agreement.	✓ Formal description of the key security roles and responsibilities. ✓ Proof of employment's changes communication. ✓ Proof of logical and physical access review. ✓ Proof of organisation assets return.
2	✓ Exit interviews are performed in order to ensure that individuals understand any security constraints imposed by being a former employee and that proper accountability is achieved for all smart grid information system-related property.	✓ Proof of exit interviews.
3	✓ Automated process review access permissions that are initiated by personnel changes.	✓ Proof of automated process.

SM 4.3 Security and awareness program. The provider should establish and maintain a security awareness program across the organisation.		
Level	**Practices**	**Evidence**
1	✓ A security awareness and training program is available and approved by management. ✓ Basic security awareness briefings are provided to smart grid system users on a regular basis. ✓ Records of the awareness activities for each user are maintained by the organisation.	✓ Documented awareness and training program containing at least: ○ Objectives, roles, and responsibilities; ○ Scope; ○ Procedures that supports the awareness and training program. ✓ Proof of security awareness briefings activities. ✓ Records of individual awareness activities.
2	✓ Changes on smart grid information systems and procedures are reviewed for	✓ The last planned review has been done according with the review process.

SM 4.3 Security and awareness program. The provider should establish and maintain a security awareness program across the organisation.		
Level	**Practices**	**Evidence**
	inclusion in the organisation security awareness and training program. ✓ The awareness and training program is regularly reviewed and revised, based on the review and new insights, new risk aspects, incidents that occurred. ✓ Contents of security awareness briefings are based on specific requirements of the organization and the smart grid information system to which personnel have authorized access.	✓ Meeting minutes of review sessions. ✓ List of contacts with security groups and associations. ✓ Documented contents of security awareness briefings.
3	✓ Contacts and communication channels with security groups and associations have been established in order to stay up to date with the latest recommended security practices, techniques, and technologies. ✓ Practical exercises that simulate actual cyber-attacks are included in security awareness briefings.	✓ List of contacts with security groups and associations. ✓ Documented communication channels. ✓ Records of simulated actual cyber-attacks. ✓ Meeting minutes of review sessions.

SM 4.4 Security training and certification of personnel. The provider should establish and maintain security training and personnel certification programmes, taking into account its needs based on their roles and responsibilities.		
Level	**Practices**	**Evidence**
1	✓ Basic security training activities are provided to smart grid system users before authorizing access to the smart grid information system, when required by smart grid information system changes or on a defined frequency. ✓ Records of the training activities for each user are maintained by the organisation.	✓ Proof of training activities. ✓ Records of individual training activities.
2	✓ Contents of security training are based on assigned roles and responsibilities and specific requirements of the organization and the smart grid information system to which personnel have authorized access.	✓ Documented contents of security training.
3	✓ Recognised security certifications are provided to organisation personnel.	✓ Results of individual certification process.

4.5 Domain 5: Incident response & information knowledge sharing

Control Objective
The provider has established and maintains an incident response and information knowledge sharing process that prevents, resolves and recovers from cyber events, effectively containing the damage, and allows sharing cyber security information for internal and external entities.

SM 5.1 Incident response capabilities.
The provider should establish and maintain capabilities to respond against cyber security incidents.

Level	Practices	Evidence
1	✓ Smart grid information system and network incidents are tracked and documented by the organisation. ✓ Smart grid information system and network incidents security incidents are reported by the organisation.	✓ Documented security incidents. ✓ Records of reported security incidents.
2	✓ An incident response program approved by management is developed and maintained in the organisation. ✓ Personnel involved in the incident response program are trained in their incident response roles and responsibilities with respect to the smart grid information system and receive refresher training on an organization-defined frequency. ✓ An incident handling capability for security incidents is implemented and reviewed by the organisation.	✓ Documented roles and responsibilities containing at least: ○ Roles and responsibilities in relation to various types of incidents; ○ Responsible personnel to lead the response effort if an incident occurs; ○ Response teams need to be formed. ✓ Management commitment with the incident response program. ✓ Records of individual training activities. ✓ Description of the incident handling capability containing at least the following procedures: ○ Preparation; ○ Detection; ○ Analysis; ○ Containment; ○ Mitigation; ○ Recovery.
3	✓ Corrective measures are reviewed to ensure their effectiveness and	✓ Meeting minutes of review sessions.

SM 5.1 Incident response capabilities. The provider should establish and maintain capabilities to respond against cyber security incidents.		
Level	**Practices**	**Evidence**
	adequately implementation. ✓ Lessons learned from incident handling activities are incorporated to incident response procedures. ✓ Regular cyber exercises and related results to test the incident response effectiveness are scheduled and documented.	✓ Records of cyber exercises.

SM 5.2 Vulnerability assessment. The provider should establish and maintain vulnerability assessment activities on the smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ Smart grid information systems are monitored and evaluated on a regular basis to identify vulnerabilities that might affect the security of a smart grid information system.	✓ Documented vulnerability scans reports.
2	✓ A single point of contact and communication channels for information security related issues with manufacturers or vendors have been identified. ✓ Security vulnerabilities of the legacy systems and technologies related are part of the vulnerability assessment activities.	✓ List of manufactures single point of contact. ✓ Proof of vulnerability assessment activities in legacy systems.
3	✓ Information obtained from the vulnerability scanning process is shared with designated personnel throughout the organisation and authorities to help eliminate similar vulnerabilities in other smart grid information systems.	✓ Records of vulnerabilities information sharing.

SM 5.3 Vulnerability management. The provider should establish and maintain an appropriate vulnerability management plan in order to manage vulnerabilities on smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ A vulnerability management plan that manages the testing, installation and documentation of security patches and system updates have been established and documented.	✓ Documented vulnerability management plan.
2	✓ The installation and de-installation of patches and updates is done manually	✓ Approved documented actions on smart grid information systems.

SM 5.3 Vulnerability management. The provider should establish and maintain an appropriate vulnerability management plan in order to manage vulnerabilities on smart grid information systems.		
Level	**Practices**	**Evidence**
	by authorized and trained staff and authorized by the system owner.	
3	✓ The installation or de-installation of patches is reviewed to ensure the adequately implementation of the defined actions. ✓ Exceptions to defined actions and approved mitigating actions are identified and documented.	✓ Documented vulnerability management plan revisions. ✓ Documented and approved exceptions to the defined actions containing the alternative controls in place to ensure the confidentiality, availability and integrity of the smart grid information systems.

SM 5.4 Contact with authorities and security interest groups. The provider should establish and maintain contacts with authorities and security interest groups to be aware of vulnerabilities and threats.		
Level	**Practices**	**Evidence**
1	✓ Contacts and communication channels with relevant authorities have been identified and established.	✓ List of authorities contacts containing at least: ○ National and international agencies together with structures for co-operation for the protection of critical infrastructures; ○ National and international CERT organizations; ○ Disaster control organizations and disaster-relief teams. ✓ Documented communication channels.
2	✓ Contacts and communication channels with corresponding local, regional and national meteorological services and corresponding information services have been identified and established. ✓ Contacts and communication channels with security interest groups in order to be up-to-date regarding cyber security practices on smart grids have been identified and established.	✓ List of contact persons for meteorological services. ✓ List of meteorological information services subscribed. ✓ List of contacts with security groups and associations. ✓ Documented communication channels.
3	✓ Cross-industry incident information exchange and cooperation to learn from the experiences of others in encouraged and promoted.	✓ Records of information exchange and cooperation activities. ✓ Documented communication channels.

4.6 Domain 6: Audit and accountability

Control Objective:
The provider has established and maintained an audit and accountability process that enables sufficient logging capabilities in the smart grid systems and components and provides valuable log data for analysis.

SM 6.1 Auditing capabilities.
The provider should establish and maintain auditing capabilities on the smart grid Information systems and components.

Level	Practices	Evidence
1	✓ A list of smart grid information systems and components auditable events based on the risk assessment activities has been identified and established. ✓ Where applicable and technically feasible smart grid information systems and components are configured to produce audit records of the list of events identified previously.	✓ List of auditable events. ✓ Audit records containing at least: ○ Date and time of the event; ○ Component of the smart grid information system where the event concurred; ○ Type of event; ○ User/subject identity; ○ Outcome of the event.
2	✓ The list of auditable events includes the execution of privileged functions in the smart grid information systems and components. ✓ A set of actions have been identified and defined in case of audit processing failures.	✓ List of privileged auditable events. ✓ Documented defined set of actions in case of audit processing failures.
3	✓ The list of auditable events is revised based on current threat data, assessment of risk, and post-incident analysis. ✓ Audit records generated by smart grid information systems and components are centrally managed. ✓ Alternative requirements or countermeasures are identified when audit records cannot be deployed for technical reasons.	✓ The last planned review has been done according with the review process. ✓ Meeting minutes of review sessions. ✓ Proof of centrally audit records management. ✓ Documented alternative countermeasures for audit records.

SM 6.2 Monitoring of smart grid information systems. The provider should establish and maintain monitoring activities on the smart grid Information systems and components.		
Level	**Practices**	**Evidence**
1	✓ Smart grid information systems and components audit records are reviewed and analysed for indication of inappropriate or unusual activity on a regular basis.	✓ Proof of reviewed action on smart grid information system and components audit records.
2	✓ Findings on smart grid information system and components audit records are communicated to the designed management authority.	✓ Proof of audit findings communications. ✓ Documented communication channels.
3	✓ Automated mechanism to integrate audit review, analysis, and reporting have been identified and established. ✓ Audit information is correlated across different repositories to gain organisation-wide situational awareness.	✓ Documented defined automated mechanism.

SM 6.3 Protection of audit information. The provider should protect the audit information generated.		
Level	**Practices**	**Evidence**
1	✓ An audit storage capacity is defined for each smart grid information system and components. ✓ An audit retention time period is defined for audit records.	✓ Documented defined audit storage capacity. ✓ Documented defined audit retention time period.
2	✓ Smart grid information system and components audit records are protected for unauthorized access, modification or deletion. ✓ Smart grid information systems and components audit records are time-stamped using agreed accurate time sources.	✓ Documented defined security measures to protect audit records for unauthorized access, modification or deletion. ✓ Documented defined accurate time sources.
3	✓ Directly or indirectly interconnected systems with external partners uses a common and agreed time sources (e.g. Central European Time (CET) or Coordinated Universal Time (UTC)). ✓ Use of non-internet synchronized NTP server or digitally signed NTP time messages.	✓ Documented agreed time sources. ✓ Documented defined NTP systems used.

4.7 Domain 7: Continuity of operations

Control Objective:
The provider has established and maintains a continuity of operations process that allows continuing or resuming operations of a smart grid information system in the event of disruption of normal system operation.

SM 7.1 Continuity of operations capabilities. The provider should establish and maintain capabilities to ensure essential functions after disruption events on smart grid Information systems.		
Level	**Practices**	**Evidence**
1	✓ A continuity operations plan approved by management is developed in the organisation. ✓ Disruptions root causes are analysed and reported to the management.	✓ Documented continuity operations plan containing at least: ○ Roles and responsibilities; ○ Scope of the plan; ○ Capabilities to recover and reconstitute the smart grid information system to a known secure state after a disruption, compromise, or failure; ○ Compensating security controls for the organisation-defined circumstances that inhibit recovery to a known secure state; ○ Fail-safe procedure upon the loss of communications with other smart grid information systems or the loss of the smart grid information system itself; ○ Backup procedures; ○ Agreements with third parties services or defined alternate supply services like alternate power supply resources. ✓ Management commitment with the continuity operations plan. ✓ Records of the management review. ✓ Documented alternate power supply.
2	✓ Personnel involved in the continuity operations plan are trained in their roles and responsibilities with respect to the smart grid information system and receive refresher training on an organization-defined frequency. ✓ Operating safety functions are identified and protected in accordance with	✓ Records of individual training activities. ✓ Documented results of the continuity of operations test activities. ✓ Last planned review has been done according with the review process. ✓ Meeting minutes of review sessions.

SM 7.1 Continuity of operations capabilities. The provider should establish and maintain capabilities to ensure essential functions after disruption events on smart grid Information systems.		
Level	**Practices**	**Evidence**
	sector-specific standards and legal requirements. ✓ The continuity of operations plan is tested and updated on a regular basis. ✓ A long-term alternate power supply for the smart grid information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source is provided by the organisation.	✓ Documented alternate power supply. ✓ Documented protection measures for operating safety functions such as: o Use of dedicated, isolated communication systems for the transmission of safety related data communications; o Independency of operating safety functions.
3	✓ Requirements for an alternate storage site are identified and evaluated by the organisation. ✓ Requirements for an alternate control centre are identified and evaluated by the organisation. ✓ Requirements for less likely attacks but with a high impact (e.g. electromagnetic pulse) are identified and evaluated by the organisation.	✓ Documented requirements for an alternate storage site containing at least: o Smart grid information system backups and the transfer rate of backup information to the alternate storage; o Potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and explicit mitigation actions; o Geographically locations (e.g. city, close to the see, etc.); o Agreement with third parties. ✓ Documented requirements for an alternate control centre containing at least: o Equipment, telecommunications, and supplies required; o Potential accessibility problems at the alternative control centre in the event of an area-wide disruption or disaster and explicit mitigation actions; o Geographically locations; o Agreement with third parties. ✓ Documented smart grid information system configuration in alternate systems. ✓ Documented requirements for less likely attacks but with a high impact.

SM 7.2 Essential communication services. The provider should establish, maintain and test essential/emergency communication services in case of major disasters.		
Level	**Practices**	**Evidence**

SM 7.2 Essential communication services. The provider should establish, maintain and test essential/emergency communication services in case of major disasters.		
Level	**Practices**	**Evidence**
1	✓ Essential communication links are identified and established with internal/external emergency teams and organisations.	✓ Documented communication channels covering the following stakeholders: ○ Operating and emergency staff in central or decentralized locations; ○ Internal and external crisis management; ○ Power stations; ○ Distributed energy producers; ○ Transmission and distribution grid operators; ○ Meteorological organizations; ○ Flood prevention organizations; ○ Fire service organizations; ○ Disaster relief organizations; ○ Safety authorities; ○ Telecommunication service providers; ○ Medical institutions; ○ Other national or local organizations that handle essential public services.
2	✓ Essential data and communication links with emergency control systems and related subcomponents and emergency alarm and monitoring systems and related subcomponents are identified and established.	✓ Documented communication channels.
3	✓ Requirements for an alternate communication services are identified and evaluated by the organisation.	✓ Documented requirements for an alternate control centre containing at least: ○ Agreements to permit the resumption of operations for the safe operation of the smart grid information system within an organization-defined time period; ○ Primary and alternate telecommunication service agreements containing priority-of-service provisions in accordance with the organisation's availability requirements.

4.8 Domain 8: Physical security

Control Objective:
The provider has established and maintains a physical security program that restricts the access to smart grid information systems and components only to authorized personnel.

SM 8.1 Physical security.
The provider should establish and maintain the appropriate physical security of the smart grid facilities/components/systems.

Level	Practices	Evidence
1	✓ Security perimeters are used to protect areas that contain information and information processing facilities. ✓ Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access. ✓ Physical security controls are designed and applied to offices, rooms and facilities. ✓ Physical protection and guidelines for working in secure areas are designed and applied. ✓ Access points such as delivery and loading area and other points where unauthorized persons may enter the premises are controlled.	✓ Documented diagram of security perimeters. ✓ Documented description of entry controls. ✓ Documented diagram with special security requirements. ✓ Documented physical protection controls against natural or man-made disaster. ✓ Documented physical protection controls and guidelines on working areas. ✓ Documented diagram of delivery and loading areas.
2	✓ Physical access controls is considered for peripheral sites where sensitive process control equipment is located. ✓ Measures to ensure the physical security of control centres, where central control systems such as control servers, HMI and supporting systems are housed, are designed, developed and applied. ✓ Measures to ensure the physical security of equipment rooms where control system facilities used by providers are located, are designed, developed and implemented.	✓ Documented diagram and description of entry controls on peripheral sites. ✓ Documented diagram on control centres. ✓ Documented diagram on equipment rooms.
3	✓ Measures to ensure physical security of the peripheral sites where control system facilities used by providers are located, are designed, developed and applied.	✓ Documented diagram and description of entry controls on peripheral sites. ✓ Documented mitigation measures on peripheral sites.

SM 8.1 Physical security. The provider should establish and maintain the appropriate physical security of the smart grid facilities/components/systems.		
Level	**Practices**	**Evidence**
	✓ Mitigation controls have been identified on equipment where is not possible to achieve a comprehensive level of physical protection for unmanned peripheral sites.	

SM 8.2 Logging and monitoring physical access. The provider should establish and maintain capabilities for logging and monitoring the physical access to the smart grid facilities/components taking into account the criticality of the facility.		
Level	**Practices**	**Evidence**
1	✓ A list of personnel with authorized access to facilities containing smart grid information systems and appropriate authorization credentials (e.g., badges, identification cards) is maintained by the organisation. ✓ A designated official within the organisation to review and approve the list of personnel with authorized access has been identified. ✓ Visitors are authenticated before authorizing access to the facility. ✓ Visitors are escorted as required according to security policies and procedures.	✓ List of personnel with authorized access. ✓ Formal appointed of the backup person. ✓ List of authorized visitors.
2	✓ Visitor's access records to the facility are maintained by the organisation. ✓ The Physical access to the smart grid information system is monitored by the organisation.	✓ Records of visitors access to the facility. ✓ Documented description of monitoring equipment.
3	✓ Physical access records are reviewed on a regular basis. ✓ Physical access records are retained as dictated by applicable regulations or based on an organization-defined period by approved policy.	✓ Proof of record's review. ✓ Documented defined period of retention.

SM 8.3 Physical security on third party premises. The provider should protect equipment located outside of the organisations' own grounds or premises in areas that are the responsibility of other utilities against physical and environmental threats.		
Level	**Practices**	**Evidence**
1	✓ Equipment installed on the third party's premises owned by other provider (e.g. transfer station) is sited in protected areas where physical and environmental security is addressed as described in previous security measures. ✓ Equipment installed on the customer premises is protected against physical and environmental threats.	✓ Documented security controls containing at least: ○ Limits of the responsibility and interface with other providers is identified and specified; ○ Agreements with the other organization for the supply of supporting infrastructure services. ✓ Documented security controls on customer premises containing at least: ○ Limits of the responsibility and interface with customers is identified and specified. ○ Alarms and tamper protection measures.
2	✓ Equipment installed on the third party's premises is isolated from other third party equipment. ✓ The status of the interconnected interfaces is monitored.	✓ Documented diagram of equipment installed on third parties premises. ✓ Records of interface monitoring activities.
3	✓ Auditing activities to ensure the implementation of necessary security requirements in the third party are performed by the organisation. ✓ Agreements are in place in order ensure the timely access to the equipment installed on the third party's premises under special defined circumstances	✓ Documented results of auditing activities. ✓ Documented agreements with third parties.

4.9 Domain 9: Information systems security

Control Objective:
The provider has established and maintains information systems security controls that ensure that the smart grid information systems and components are logically accessed only by authorized entities and that its information is properly protected.

SM 9.1 Data security.
The provider should implement security requirements in order to protect the information on smart grid information system.

Level	Practices	Evidence
1	✓ Minimum security requirements are defined for stored data.	✓ Documented minimum security requirements for stored data.
2	✓ Information is classified in terms of value, legal requirements, sensitivity and criticality to the organisation. ✓ An appropriate set of procedures for information labelling and handling should be developed and implemented in accordance with the classification scheme adopted by the organisation.	✓ Documented information classification levels. ✓ Documented set of security requirements based on information classification levels. ✓ Identify labelling/handling procedures for different categories of information defined.
3	✓ Detailed procedures for the disposal or destruction of smart grid information system information are defined. ✓ Information that requires special control or handling is reviewed on a periodic basis to validate that special handling is still required.	✓ Documented procedures for the disposal or destruction of data. ✓ The last planned review has been done according with the review process. ✓ Meeting minutes of review sessions.

SM 9.2 Account management.
The provider should establish and maintain system/groups/user accounts on smart grid information systems.

Level	Practices	Evidence
1	✓ Smart grid information system accounts have been identified and managed. ✓ Management approval is required prior to establishing accounts. ✓ Smart grid information system accounts are reviewed on a regular basis. ✓ Account managers are notified when smart grid information system users are terminated, transferred, or smart grid information system usage changes.	✓ Documented access management procedure containing at least: ○ Account types; ○ Access rights; ○ Privileges. ✓ Proof of management approval prior establishing accounts. ✓ Proof of information system account review. ✓ Proof of accounts notification to account managers.
2	✓ The use of guest/group accounts is monitored by the organisation. ✓ Smart grid information system automatically disables inactive accounts after an organization-defined time period. ✓ The account creation, modification, disabling, and termination actions is recorded on smart grid information systems.	✓ Results of monitoring activities on guest/anonymous/group accounts. ✓ Records of account actions.

SM 9.2 Account management. The provider should establish and maintain system/groups/user accounts on smart grid information systems.		
Level	**Practices**	**Evidence**
3	✓ Automated mechanism is employed to support the management of smart grid information system accounts. ✓ Smart grid information system automatically terminates temporary and emergency accounts after an organization-defined time period for each type of account.	✓ Documented description on automated mechanism used. ✓ Proof of terminated temporary and emergency accounts.

SM 9.3 Logical access control. The provider should enforce logical access to authorised entities on smart grid information systems and security perimeters.		
Level	**Practices**	**Evidence**
1	✓ Allowed methods of access control to the smart grid information system are identified and documented. ✓ Smart grid information system enforces assigned authorizations for controlling access to the smart grid information system in accordance with organization-defined policy. ✓ User accounts are granted with the most restrictive set of rights and privileges or access needed for the performance of specified tasks. ✓ Smart grid information system accounts are temporarily disabled after a defined limit of consecutive invalid login attempts.	✓ Documented methods of access control containing at least: ○ Authentication type; ○ Authorization schema. ✓ List of smart grid information system users and related access rights. ✓ Records of disabled accounts after a defined limit of consecutive invalid login attempts.
2	✓ Smart grid information system functions are separated through assigned access authorizations. ✓ Security functions are restricted to the least amount of users necessary to ensure the security of the smart grid information system.	✓ List of authorized users who can access to security functions.
3	✓ Alternative requirements or countermeasures are identified when allowed methods of access control cannot be implemented (e.g. legacy system that cannot support a strong password policy). ✓ Restrictions in the number of concurrent sessions are defined and implemented by the organisation.	✓ Documented alternative countermeasures such as: ○ Secure unique password; ○ Real-time logging and recording of unsuccessful login attempts; ○ Real-time alerting of a management authority for the smart grid information system when the number of defined consecutive invalid access attempts is exceeded.

SM 9.3 Logical access control. The provider should enforce logical access to authorised entities on smart grid information systems and security perimeters.		
Level	**Practices**	**Evidence**
		✓ Documented defined number of concurrent sessions.

SM 9.4 Secure remote access. The provider should establish and maintain secure remote access where applicable to smart grid information systems.		
Level	**Practices**	**Evidence**
1	✓ Allowed methods of remote access to smart grid information system are identified and documented. ✓ Restrictions in the use of wireless technologies are identified and documented. ✓ Wireless access to smart grid information system is protected using secure authentication methods and encryption controls.	✓ Documented method of remote access. ✓ Documented restrictions in the use of wireless technologies. ✓ Documented authentication and encryption methods.
2	✓ Remote access connections are approved and monitored. ✓ The confidentiality and integrity of the remote access connections are secured by secure cryptographic controls. ✓ Remote sessions are terminated at the end of the session or after a defined period of inactivity.	✓ Records of monitoring activities.
3	✓ Automated mechanisms are employed to monitor and control remote access connections.	✓ Documented description of automated mechanism.

SM 9.5 Information security on information systems. The provider should establish and maintain appropriate information security capabilities on information systems, to provide protection against malware, viruses and other common threats.		
Level	**Practices**	**Evidence**
1	✓ Malicious code protection mechanisms are implemented by the organisation on the smart grid information system. ✓ The malicious code protection mechanisms are maintained up-to-date. ✓ Malicious code protection mechanisms perform periodic scans on the smart	✓ Documented malicious code protection mechanisms. ✓ Records of recent updates of malicious code protection mechanisms. ✓ Records of periodical scans.

SM 9.5 Information security on information systems. The provider should establish and maintain appropriate information security capabilities on information systems, to provide protection against malware, viruses and other common threats.		
Level	**Practices**	**Evidence**
	grid information systems.	
2	✓ The malicious code protection mechanisms are centrally managed. ✓ Smart grid information system prevents users from circumventing malicious code protection capabilities. ✓ Spam protection mechanisms are employed at system entry points and at workstations, servers, or mobile computing devices on the network.	✓ Documented description of centrally management tools. ✓ Documented spam protection mechanism. ✓ Use of whitelisting solutions, which restrict the execution of non-approved software and code.
3	✓ Alternative requirements or countermeasures are identified when malicious code protection cannot be deployed for technical reasons.	✓ Documented alternative countermeasures such as: ○ Securing of all physical and logical data interfaces; ○ Network isolation and implementation of segmented network security zones that limit the impact of a malware incident; ○ Comprehensive system hardening measures to minimize the risk of malware incidents.

SM 9.6 Media handling. The provider should establish and maintain secure procedures for the access, storage, distribution, transport, sanitization, destruction and disposal of the media assets.		
Level	**Practices**	**Evidence**
1	✓ A media protection policy that addressed the use and protection requirements for media assets is available and approved by management. ✓ The access, control, sharing, copying, transmittal and distribution of media assets is aligned with the information classification levels and protection required measures defined in the media protection policy. ✓ Media assets are marked in accordance with organisation-defined policy and procedures.	✓ Approved media protection policy containing at least: ○ Objectives, roles, and responsibilities for the media protection security program; ○ Scope of the media protection security program; ○ Management commitment with the media protection policy; ○ Information classification levels for media assets; ○ Protection required commensurate with the organisation information classification levels for media assets. ✓ Use of external and internal marking labels on media assets. ✓ Use of internal marking labels on smart grid information system output.

SM 9.6 Media handling. The provider should establish and maintain secure procedures for the access, storage, distribution, transport, sanitization, destruction and disposal of the media assets.		
Level	**Practices**	**Evidence**
2	✓ The media protection policy is regularly reviewed at planned intervals of significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. ✓ The organisation use secure procedures to sanitize the information from media assets before the disposal or re-use. ✓ Sanitization equipment is tested in order to verify its correct performance on a regular basis.	✓ Last planned review has been done according with the review process. ✓ Meeting minutes of review sessions. ✓ Documented test results for sanitization equipment. ✓ Documented secure procedures in order to remove the information from media assets.
3	✓ The media protection policy is regularly reviewed at planned intervals of significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. ✓ Smart Grid information system media is physically managed and stored in protected areas based on its information classification level. ✓ Media assets are protected during transport outside controlled areas using organisation-defined security measures.	✓ Use of protected areas for sensitive smart grid information system media. ✓ Documented organisation-defined security measures for the transport of media assets covering the accountability of media assets during the transport outside controlled areas and restricting the transport of media assets only for authorised personnel.

4.10 Domain 10: Network security

Control Objective:
The provider has established and maintains a secure network engineering program that prevents security controls from being circumvented.

SM 10.1 Secure network segregation. The provider should establish and maintain a segregated network for the smart grid information system.		
Level	**Practices**	**Evidence**
1	✓ Smart grid information system management functionality is separated from smart grid information system user functionality.	✓ Proof of system management and user functionality partitioning.

SM 10.1 Secure network segregation. The provider should establish and maintain a segregated network for the smart grid information system.		
Level	**Practices**	**Evidence**
2	✓ Where applicable and technically feasible the network infrastructure of process control systems is divided into multiple zones with different functions and protection requirements. ✓ Where applicable and technically feasible the networks and distributed systems should be divided into independent horizontal segments. ✓ Where applicable and technically feasible a specific network for patch management functions (e.g. testing) is defined.	✓ Documented network design and configuration containing at least: ○ Physical, virtual and logical network connections; ○ Network protocols and ports; ○ Network perimeter components; ○ Technical and operational domains.
3	✓ Network zones and network segments are separated by firewalls, filtering routers or gateways.	✓ Documented description of protection network devices.

SM 10.2 Secure network communications. The provider should establish and maintain secure communications across the segregated network.		
Level	**Practices**	**Evidence**
1	✓ The smart grid information system management communication path is physically or logically separated from the telemetry/data acquisition services communication path.	✓ Proof of communication partitioning.
2	✓ Where technically feasible, smart gird information systems (including SCADA components) only use secure communication standards and protocols which provide integrity checks, authentication and, if applicable, encryption. ✓ Secure communications are used for remote administration or transmission of user log-on information. ✓ Network connections to external networks are deployed only using communication protocols approved by the provider and in compliance with the security policies in effect. ✓ External smart grid information system and communication connections are identified and protected from tampering or damage.	✓ List of implemented communication standards and protocols. ✓ List of identified external connections.
3	✓ Smart grid information system routes all remote accesses through a limited	✓ Documented list of authorized control system commands and messages.

SM 10.2 Secure network communications. The provider should establish and maintain secure communications across the segregated network.		
Level	**Practices**	**Evidence**
	number of managed access control points. ✓ Only authorized communications and information flows are exchanged over the communication link. ✓ Where technically feasible, intrusion detection systems and intrusion prevention systems (signatures based or behavioural) are implemented on smart gird information systems (including SCADA components) and/or network (especially in field devices networks). ✓ Network connections to external networks are routed via especially hardened application proxies, which are located in a separate network zone (demilitarized zone) specifically for this purpose.	✓ Documented list of authorized information flows. ✓ Documented description of protection network devices.

5 Catalogue of security measures

This section contains a summary of the aboved described domains and cyber security measures.

Domain	List of Security Measures
Security governance & risk management	Information security policy
	Organisation of information security
	Information security procedures
	Risk management framework
	Risk assessment
	Risk treatment plan
Third parties management	Third party agreements
	Monitoring third parties services and validating solutions against predefined acceptance criteria
Secure lifecycle process for smart grid components and operating procedures	Security requirements analysis and specification
	Inventory of smart grid components/systems
	Secure configuration management of smart grid components/systems
	Maintenance of smart grid components/systems
	Software/firmware upgrade of smart grid components/systems
	Disposal of smart grid components/systems
	Security testing of smart grid components/systems
Personnel security, awareness and training	Personnel screening.
	Personnel changes
	Security and awareness program
	Security training and certification of personnel
Incident response & information knowledge sharing	Incident response capabilities
	Vulnerability assessment
	Vulnerability treatment
	Contact with authorities and security interest groups
Audit and accountability capability	Auditing capabilities
	Monitoring of smart grid information systems
	Protection of audit information
Continuity of operations capability	Continuity of operations capabilities
	Essential communication services
Physical security	Physical security
	Logging and monitoring physical access
	Physical security on third party premises
Information systems security	Data Security
	Account management
	Logical access control
	Secure remote access
	Information security on information systems
	Media handling
Network security	Secure network segregation
	Secure network communications

6 Mapping with ISO/IEC 27002, NISTIR 7628 and ISO/IEC TR 27019

This section contains a mapping between the between the defined security measures and the standards ISO/IEC-27002, NISTIR-7628 and ISO/IEC TR 27019.

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
Security governance & risk management	Information security policy	5.1.1 Information security policy document 5.1.2 Review of the information security policy 6.1.1 Management commitment to information security	SG.PM-1 Security Program Management SG.PM-3: Senior Management Authority
	Organisation of information security	6.1.2 Information security coordination 6.1.3 Allocation of information security responsibilities 8.1.1 Roles and responsibilities	SG.PM-1 Security Program Management SG.PM-3: Senior Management Authority SG.PM-8: Management Accountability SG.PM-19 Security Roles SG.AC-6: Separation of Duties
	Information security procedures	15.2.1 Compliance with security policies and standards	SG.PM-1 Security Policy and Procedures
	Risk management framework	12.6 Technical Vulnerability Management	SG.PM-5 Risk Management SG.RA-2 Risk Management Plan
	Risk assessment	4.1 Assessing security risks	SG.RA-1 Risk Assessment Policy and Procedures SG.RA-3: Security Impact Level SG.RA-4: Risk Assessment SG.RA-5: Risk Assessment Update
	Risk treatment plan		SG.RA-2 Risk Management Plan
Third parties management	Third party agreements	6.1.5 Confidentiality agreements 6.2.1 Identification of risks related to external parties 6.2.3 Addressing security in third party agreements 14.1.2 Business continuity and risk assessment	SG.AC-1: Access Control Policy and Procedures SG.CP-8: Alternate Telecommunication Services SG.CP-9: Alternate Control Center SG.PS-7 Contractor and Third-Party Personnel Security SG.PS-9: Personnel Roles SG.SA-2 Security Policy for Contractors and Third Parties SG.SA-4: Acquisitions
	Monitoring third parties services and validating solutions against predefined acceptance criteria	10.2 Third party service delivery management	SG.AU-1 Audit and Accountability SG.AU-11: Conduct and Frequency of Audits

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
Secure lifecycle process for smart grid components and operating procedures	Security requirements analysis and specification	12.1.1 Security requirements analysis and specification	SG.SA-8 Security Engineering Principles
	Inventory of smart grid components/systems	7.1.1Inventory of assets	SG.CM-2: Baseline Configuration SG.CM-8: Component Inventory SG.ID-3: Information Handling SG.ID-5: Automated Labelling, SG.MP-2: Media Sensitivity Level SG.MP-3: Media Marking, SG.PL-3: Rules of Behaviour SG.PM-4: Security Architecture SG.PS-6: Access Agreements SG.RA-3: Security Impact Level
	Secure configuration management of smart grid components/systems	7.1.2 Ownership of assets 7.1.3 Acceptable use of assets B.1.1.1.9 Secure Standard Configuration (from ISO/IEC TR 27019)	SG.CM-2 Baseline Configuration SG.CM-3: Configuration Change Control SG.CM-4: Monitoring Configuration Changes SG.CM-5: Access Restrictions for Configuration Control SG.CM-6: Configuration Settings SG.CM-8 Component inventory SG.CM-10: Factory Default Settings Management SG.CM-11 Configuration Management Plan
	Maintenance of smart grid components/systems	9.2.4 Equipment maintenance	SG.MA-1: Smart Grid Information System Maintenance Policy and Procedures SG.MA-3 Smart Grid information system maintenance SG. MA-4: Maintenance Tools SG.MA-6: Remote Maintenance SG.MA-7: Timely Maintenance SG.PL-5: Security-Related Activity Planning
	Software/firmware upgrade of smart grid components/systems	12.5.2 Technical review of applications after operating system changes 12.5.3 Restrictions on changes to software packages 12.6.1 Control of technical vulnerabilities 13.1.2. Reporting security weaknesses	SG.SI-2 Flaw Remediation

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
	Disposal of smart grid components/systems	9.2.6 Secure disposal or re-use of equipment 9.2.7 Removal of property	SG.CM-9 Addition, removal, and disposal of equipment SG.MA-3: Smart Grid Information System Maintenance SG.MP-6: Media Sanitization and Disposal
	Security testing of smart grid components/systems	10.1.4 Separation of development, test, and operational facilities	SG.CM-2 Baseline Configuration SG.CA-2 Security Assessments SG.RA-6: Vulnerability Assessment and Awareness, SG.SA-3: Life-Cycle Support SG.SA-9: Developer Configuration Management SG.SA-10: Developer Security Testing SG.SI-6: Security Functionality Verification SG.SI-7: Software and Information Integrity
Personnel security, awareness and training	Personnel screening.	8.1.2 Screening 8.1.3 Terms and conditions of employment	SG.PS-3 Personnel Screening
	Personnel changes	8.3 Termination or change of employment 8.3.1 Termination responsibilities 8.3.2 Return of assets 8.3.3 Removal of access rights	SG.AC-3: Account Management SG.PE-3: Physical Access SG.PS-4: Personnel Termination SG.PS-5: Personnel Transfer SG.SA-2: Security Policies for Contractors and Third Parties
	Security and awareness program	8.2.2 Information security awareness, education, and training 8.2.3 Disciplinary process	SG.AT-1 Awareness and Training Policy and Procedures SG.AT-2 Security awareness SG.AT-4: Security Awareness and Training Records
	Security training and certification of personnel		SG.AT-3 Security Training SG.AT-6: Security Responsibility Testing SG.CP-4: Continuity of Operations Training SG.PS-9: Personnel Roles

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
Incident response & information knowledge sharing	Incident response capabilities	13 Information security incident management	SG.IR-1 Incident Response Policy and Procedures SG.IR-2 Incident Response Roles and Responsibilities SG.IR-3 Incident Response Training SG.IR-4 Incident Response Testing and Exercises SG.IR-5 Incident Handling SG.IR-6: Incident Monitoring SG.IR-7: Incident Reporting SG.IR-8: Incident Response Investigation and Analysis SG.IR-11: Coordination of Emergency Response
	Vulnerability assessment		SG.RA-4 Risk Assessment SG.RA-6 Vulnerability Assessment and Awareness SG.CA-6: Continuous Monitoring SG.SA-10: Developer Security Testing
	Vulnerability treatment	12.6.1 Control of technical vulnerabilities	SG.SA-8 Security Engineering Principles SG.RA-6 Vulnerability Assessment and Awareness SG.SA-7: User-installed Software SG.SI-2: Flaw Remediation
	Contact with authorities and security interest groups	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups	SG.AT-5 Contact with Security Groups and Associations SG.ID-4: Information Exchange SG.IR-9: Corrective Action
Audit and accountability capability	Auditing capabilities	10.10.1 Audit logging 15.3.1 Information systems audit controls	SG.AU-1 Audit and Accountability Policy and Procedures SG.AU-2 Auditable Events SG.AU-3 Content of Audit Records SG.AU-4: Audit Storage Capacity SG.AU-11: Conduct and Frequency of Audits SG.AU-14: Security Policy Compliance SG.AU-15 Audit Generation

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
	Monitoring of smart grid information systems	10.10 Monitoring	SG.AU-2 Auditable events SG.AU-6 Audit Monitoring, Analysis, and Reporting SG.AU-5: Response to Audit Processing Failure SG.AU-7: Audit Reduction and Report Generation SG.CA-6: Continuous Monitoring SG.SC-7: Boundary Protection
	Protection of audit information	10.10.3 Protection of log information 15.3.2 Protection of information systems audit tools	SG.AU-4 Audit Storage Capacity SG.AU-5 Response to Audit Processing Failures SG.AU-8: Time Stamps SG.AU-9 Protecting Audit Information SG.AU-10: Audit Record Retention SG.AU-16: Non-Repudiation
Continuity of operations capability	Continuity of operations capabilities	14 Business continuity management	SG.CP-1 Continuity of Operations Policy and Procedures SG.CP-2 Continuity of Operations Plan SG.CP-3 Continuity of Operations Roles and Responsibilities SG.CP-4 Continuity of Operations Training SG.CP-5 Continuity of Operations Plan Testing SG.CP-6 Continuity of Operations Plan Update SG.CP-7 Alternate Storage Sites SG.CP-9: Alternate Control Center SG.CP-10: Smart Grid Information System Recovery and Reconstitution SG.PL-5: Security-Related Activity Planning
	Essential communication services	14.2.1 Emergency communication (from ISO/IEC TR 27019)	SG.CP-8 Alternate Telecommunication Services SG.CP-9 Alternate Control Center SG.CP-11 Fail-Safe Response SG.IR-11: Coordination of Emergency Response

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
Physical security	Physical security	9.1 Secure areas 9.1.1 Physical security perimeter 9.1.2 Physical entry controls 9.1.3 Securing offices, rooms, and facilities 9.1.4 Protecting against external and environmental threat 9.1.5 Working in secure areas 9.1.6 Public access, delivery, and loading areas 9.1.7 Securing control centres 9.1.8 Securing equipment rooms 9.1.9 Securing peripheral sites	SG.PE-1: Physical and Environmental Security Policy and Procedures SG.PE-2 Physical Access Authorizations SG.PE-3: Physical Access SG.PE-8: Emergency Shutdown Protection SG.PE-9: Emergency Power SG.PE-12: Location of Smart Grid Information System Assets
	Logging and monitoring physical access	9.2.1 Equipment siting and protection 9.2.2 Supporting utilities 9.2.3 Cabling security 9.2.6 Secure disposal or re-use of equipment	SG.PE-2: Physical Access Authorizations SG.PE-4: Monitoring Physical Access SG.PE-5: Visitor Control SG.PE-6: Visitor Records SG.PE-7: Physical Access Log Retention
	Physical security on third party premises	9.2.5 Security of equipment off-premises 9.3.1 Equipment sited on the premises of other energy utility organizations 9.3.2 Equipment sited on customer's premises 9.3.3 Interconnected control and communication systems	
Information systems security	Data Security	12.3 cryptography controls 10.7.3 Information handling procedures B.1.1.1.6 Encryption of Sensitive Data during Storage and Transmission (from ISO/IEC TR 27019)	SG.ID-3 Information Handling SG.ID-5 Automated Labelling
	Account management	11.2 User access management 11.2.2 Privilege management 11.5.1 Secure log-on procedures 11.5.4 Use of system utilities 11.5.5 Session time-out 11.5.6 Limitation of connection time	SG.AC-1: Access Control Policy and Procedures SG.AC-3 Account Management SG.AC-4: Access Enforcement

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
	Logical access control	11.1.1 Access control policy 11.2.1 User registration 11.4.2 User authentication for external connections 11.6.1 Information access restriction 11.6.2 Sensitive system isolation	SG.AC-4 Access enforcement
	Secure remote access	10.6.3 Securing process control data communication 11.4.2 User authentication for external connections 12.3.1 Policy on the use of cryptographic controls	SG.AC-2 Remote Access Policy and Procedure SG.AC-3: Account Management SG.AC-13: Remote Session Termination SG.AC-15 Remote Access SG.AC-16: Wireless Access Restrictions SG.SC-8: Communication Integrity SG.SC-9: Communication Confidentiality
	Information security on information systems	10.4 Protection against malicious and mobile code	SG.SI-3 Malicious Code and Spam Protection SG.MA-4: Maintenance Tools SG.MA-6: Remote Maintenance
	Media handling	10.7.1 Management of removable media 10.7.2 Disposal of media 10.7.3 Information handling procedures 10.7.4 Security of system administration	SG.MP-1 Media Protection Policy and Procedures SG.MP-2 Media Sensitivity Level SG.MP-3 Media Marking SG.MP-4 Media Storage SG.MP-5 Media Transport SG.MP-6 Media Sanitization and Disposal
Network security	Secure network segregation	11.4.5 Segregation in networks	SG.SC-7: Boundary Protection SG.SC-29: Application Partitioning

Domain	List of Security Measures	ISO/IEC-27002 – ISO/IEC TR 27019	NISTIR-7628
	Secure network communications	10.6.1 Network control 10.6.2 Security of network services 11.4.6 Network connection control 11.4.7 Network routing control 11.4.8 Logical coupling of external process control systems 11.7.1 Mobile computing and communications	SG.AC-2: Remote Access Policy and Procedures SG.AC-4: Access Enforcement SG.AC-15: Remote Access SG.AC-17: Access Control for Portable and Mobile Devices SG.SC-2: Communications Partitioning SC.SC-7: Boundary Protection SG.SC-8: Communication Integrity SG.SC-9 Communication Confidentiality SG.SC-18: System Connections SG.SI-4: Smart Grid Information System Monitoring Tools and Techniques

Annex I - Glossary

The appropriate security measures for smart grids have been selected using a generic terminology that is detailed below, as follows:

- **Smart grid**: an upgraded electricity network to which two-way digital communication between supplier and consumer as well as between smart grid components, intelligent metering and monitoring systems have been added. In this domain, it is important to highlight the importance of the human factor as a key component of the smart grid;
- **Smart grid information system**: reflects the following key elements:
    - Information and communications technology (ICT) components: like computer or telecommunication networks;
    - Industrial control systems: like supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC);
    - Operational Technologies: like firmware or operating systems.
- **Smart grid components:** elements or devices that represent part of the smart grid information system;
- **Media assets:** this term includes compact discs, digital video discs, erasable-programmable read-only memory and embedded assets, tapes, printed reports, and documents;
- **Provider**: stakeholder which provides services to the smart grid value chain, such as:
    - Transmission System Operator (TSO): entity responsible for managing the security of the Transmission system in real time and co-ordinate the supply of and demand for electricity;
    - Distribution System Operator (DSO)[14]: entity responsible for (a) operating, (b) ensuring the maintenance of, (c) if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems; and (d) for ensuring the long term ability of the system to meet reasonable demands for the distribution of electricity;
    - Electricity generator: legal entity that produces electric energy and puts it into the system;
    - Customer**:** entity that purchases electricity for the purpose of use;

[14] *It can be foreseen that the role of the DSO will change in the Smart Grid era as more and more local production will need to be managed taking advantage of the flexibility of local loads (e.g. related to e-mobility and heat pumps). One could say that the DSO will need to co-ordinate the local supply of and demand for electricity in more and more active distribution grids. In order to do so more ICT is needed and therefore more security requirements will apply to the DSOs.*

- Electricity market: all operations related to the purchase and sale of power energy. In the electricity market, the commodity is the electrical energy which is purchased, sold or trade on short-term.
- Prosumers: combination of the roles of consumer and producer. In the energy context is the combination of the roles generator and energy user.

- **Communication network:** platform which interconnects exchange data among all devices within the smart grid infrastructure;
- **Supervisory Control and Data Acquisition (SCADA)[15]:** systems for the control of each substation, as well as for the management of the entire smart grid network;
- **Distributed control system (DCS):** system used to monitor and control systems from the measuring instrument to the control console;
- **Cyber security:** is the preservation of confidentiality, integrity and availability of information in cyberspace;
- **Cyberspace:** is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form;
- **Domain:** in the context of this study a domain is a set of measures which have a common purpose. A domain contains two key elements:
  - Control objective**:** the desired effect of the control;
  - Appropriate security measures to fulfil the control objective. Each security measure contains the following elements:
    - Examples of the security measure which highlight how the proposed security measure has been implemented in other security frameworks;
    - Practices: provides information in order to design a certain control on the organisation;
    - Sophistication level: indicates the implementation sophistication of the measure;
    - Evidence: provides information in order to verify that an organisation has implemented the practice.

The above definitions were selected based on the taxonomy that was most used by the participants in the study, and based on observations collected during the extensive desk research performed.

[15] *A more detailed description of these elements can be found on the following document http://www.tno.nl/downloads/TNO-DV%202008%20C096_web.pdf.*

Annex II – References

European Commission (2011) Smart Grid Mandate M/490 EN, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf.

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:EN:PDF.

European Commission Task Force for Smart Grids, Expert Group 2: Regulatory recommendations for data safety, data handling and data protection report issued on February 16, 2011, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

ISO/IEC 27000 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56891.

ISO/IEC 27011: Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43751.

NISTIR 7628: Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

ISA 99, Industrial Automation and Control Systems Security, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821.

NERC CIP (North America Electric Reliability Protection Critical Infrastructure Protection) http://www.nerc.com/page.php?cid=2%7C20.

IEC 62443 Industrial communication networks: http://www.iec.ch/.

European SCADA and Control Systems Information Exchange (EuroSCSIE), https://espace.cern.ch/EuroSCSIE/default.aspx.

EU European Commission document, "A Reference Security Management Plan for Energy Infrastructure," Section B, http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf.

Risk Assessment, NIST SP 800-30, Guide for Conducting Risk Assessments, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

The U.S. Department of Energy (DOE) Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model.

European Commission recommendation of 09.03.2012 on preparations for the roll-out of smart metering systems, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20120309_smart_grids_recommendation_en.pdf;

Lockhart, B., & Gohn, B. (2011a). Utility Cyber Security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond. Boulder: Pike Research, http://www.pikeresearch.com/wordpress/wp-content/uploads/2011/11/UCS-11-Pike-Research.pdf.

ORGALIME, July 2010, http://www.orgalime.org/positions/positions.asp?id=358.

GEODE, October 2010, http://www.geode-eu.org.

ERGEG, position paper on Smart Grids, No. E10-EQS-38-05, June 2010, http://www.energyregulators.eu/portal/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_ERGEG_PAPERS/Electricity/2010/E10-EQS-38-05_SmartGrids_Conclusions_10-Jun-2010_Corrige.pdf.

Joint BEUC and ANEC, http://www.anec.org/attachments/ANEC-PT-2010-AHSMG-005final.pdf.

M441 on 12 March 2009, http://www.cen.eu/cen/Sectors/Sectors/Measurement/Pages/default.aspx.

M468 on 29 June 2010, http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm.

US Energy Policy Act of 2005, Pub. L. No 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005), http://www.gpo.gov/fdsys/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf.

US NERC Rules of Procedure. Available, http://www.nerc.com/page.php?cid=1|8|169.

Mandatory Reliability Standards for Critical Infrastructure Protection, US Federal Energy Regulatory Commission, Order No. 706, 73 FR 7368 (Feb. 7, 2008), 122 FERC 61,040, 123 FERC 61,174 (2008), http://www.ferc.gov/whats-new/comm-meet/2008/091808/E-26.pdf.

US NERC Project 2008-06, Cyber Security Order 706, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html.

US E-Government Act of 2002, Pub. L. 107-347, Title III, 116 Stat. 2899 (2002), http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm.

"Guide to NIST Information Security Documents.", http://csrc.nist.gov/publications/CSD_DocsGuide.pdf.

"Risk Management Framework," US National Institute of Standards and Technology (2002), http://csrc.nist.gov/groups/SMA/fisma/framework.html.

"Minimum Security Requirements for Federal Information and Information Systems," FIPS Publication 200, US National Institute of Standards and Technology, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

US Energy Independence and Security Act of 2007, Pub. L. 110-140 (2007), http://www.gpo.gov/fdsys/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf.

"Catalogue of Control Systems Security: Recommendations for Standards Developers," US Department of Homeland Security, U.S. Computer Emergency Readiness Team, September 2009, http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf.

Expert Group on the security and resilience of communication networks and information systems for Smart Grids,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/expert_group_smart_grid/index_en.htm.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu