SDN-µSense

Project No. 833955

Project acronym: SDN-microSENSE

Project title:

SDN - microgrid reSilient Electrical eNergy SystEm

Deliverable D3.4

Energy-related Personnel & Processes Readiness Evaluation

Programme: H2020-SU-DS-2018

Start of the project: 01.05.2019

Duration: 36 months

Editor: TECNALIA

Due date of the deliverable: 30/06/2020

Actual submission date: 03/07/2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833955

Deliverable Description:

Deliverable Name	Energy-related Personnel & Processes Readiness Evaluation
Deliverable Number	D3.4
Work Package	WP 3
Associated Task	T3.4
Covered Period	M2-M14
Due Date	M14
Completion Date	M14
Submission Date	3/7/2020
Deliverable Lead Partner	TECN
Deliverable Author(s)	AYESA, UOWM, IEIT, ESO, CEZ, UBITECH, 8BELLS, ALKYONIS, VETS, IREC, EPESA, CW, DIEL, IDENER
Version	**1.0**

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Change Control

Document History

Version	Date	Change History	Author(s)	Organisation
0.1	25/10/2019z	Document Template and objectives	Xabier Yurrebaso Iñaki Angulo	TECNALIA
0.2	3/3/2020	Section 2. User Roles. Compilation of contributions of task partners about user roles in an energy company.	Iñaki Angulo	TECNALIA
0.3	30/3/2020	Classification of User Roles and Smart Grids Assets and Threats. User Roles Description	Iñaki Angulo	TECNALIA
0.4	27/4/2020	Revision of User Roles description by the stakeholders	Jose Antonio Pérez Chloe Coral Jaime Argüelles Panagiotis Famelis.	IDENER EPESA AYESA IPTO
0.5	4/5/2020	Section 2. High level definition of the Validation Methodology.	Iñaki Angulo Xabier Yurrebaso Izaskun Santamaria	TECNALIA

		Section 4. Cybersecurity Capacity Model of an Energy Company. Section 5. Cybersecurity Personnel Competences in an Energy Company		
0.6	20/5/2020	Section 4. More information about the Maturity model is added. Section 5. More information about knowledge categories and subcategories is added.	Iñaki Angulo Marisa Escalante Izaskun Santamaria	TECNALIA
0.7	25/5/2020	Section 4. Description of the Managed Level Processes has been added. Section 5. Contributions from task partners have been added.	All	All
0.8	1/6/2020	Section 4 and 5 has been completed. Section 6 has been added	All	All
0.9	5/6/2020	First Version for Internal Review	All	All
0.10	26/6/2020	Review feedback have been incorporated in the document	Iñaki Angulo Marisa Escalante Izaskun Santamaria	TECNALIA
1.0	30/6/2020	Version 1.0 of the document	All	All

Distribution List

Date	Issue	Group
05/06/2020	Revision	AYESA, UOWM, CERTH
3/7/2020	Acceptance	AYESA, UOWM, CERTH
3/7/2020	Submission	AYESA

SAB approval

Name	Institution	Date
José Antonio Pérez	IDENER	22/06/2020

Academic and Industrial partner revision

Name	Institution	Date
Thomas Lagkas	Academic partner: UOWM	19/06/2020
Jaime Argüelles	Industrial partner: AYESA	19/06/2020

Table of contents

List of Figures

List of Tables

Acronyms

Acronym	Explanation
AMI	Advanced Metering Infrastructure
BES	Bulk Electric System
CCMM	Cybersecurity Capability Maturity Model
CSMS	Cyber Security Management System
DER	Distributed Energy Resources
DMS	Distribution Management System
DSM	Demand Side Management
DSO	Distribution System Operation
e-CF	European e-Competency Framework
ECRA	Energy Chain Risk Assessment
EMS	Energy Management System
ENISA	European Cybersecurity Agency
EPES	Electrical Power and Energy System
EV	Electric Vehicle
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IT	Information Technology
KSA	Knowledge, Skills and Abilities
NERC CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NIST NICE	National Institute of Standards and Technology – National Initiative for Cybersecurity Education
OT	Operation Technology
P-CMM	People Capacity Maturity Model
People CMM	People Capacity Maturity Model
PLC	Power Line Communication
RTU	Remote Terminal Unit
SCADA	Supervision and Control Acquisition Data System
SGAM	Smart Grid Architectural Model
TSO	Transmission System Operator

Executive Summary

There is a concern in the energy sector about the low level of cybersecurity training in the company staff, that is considered a security risk for the company and the infrastructures it operates. The standard IEC-62443-2-1, considers that security awareness for all personnel is an essential tool for reducing cybersecurity risks. Companies are aware that they need to improve cybersecurity competences of their employees, especially those that operate the most critical assets. However, cybersecurity training cannot be done in an improvised way, when the company or society has suffered some type of cyber-attack, nor can it be left to the employees' will. As such, it is necessary to institutionalise a set of processes and practices within the organization that provide employees cybersecurity awareness and training specific to their working activity.

SDN-microSENSE has developed a Cybersecurity Awareness and Training Model and an Evaluation Tool towards addressing this challenge in order to help energy companies to improve their cybersecurity training processes. The model establishes the set of processes and practices that must be institutionalised in the company to manage the cybersecurity awareness and training of its personnel. The evaluation tool helps to assess the level of maturity reached by the company in the deployment of these processes and practices. Furthermore, a competency framework has also been developed with a set of cybersecurity knowledge, skills and abilities to be adopted by the people according to their working role.

This document describes the *Cybersecurity Awareness and Training Model and the Evaluation Tool,* that is composed of three main components:

1. Cybersecurity Capability Maturity Model.
2. Cybersecurity Competency Model.
3. Evaluation tool.

Cybersecurity Maturity Model

The first component of the SDN-microSENSE Cybersecurity Awareness and Training Model is the Cybersecurity Maturity Model. In the context of the SDN-microSENSE, the Cybersecurity Maturity Model is defined as a set of processes and practices that have to be institutionalised in a company to improve the competency level of its personnel in cybersecurity aspects. The model defines 3 Maturity Levels, representing different degrees of organizational capabilities for managing and developing the training, skills, and competency processes, to generate a cybersecurity culture inside an energy company. Each maturity level, besides the Initial Level, consists of four processes, which identify the capabilities that must be institutionalized in the company to achieve a maturity level. Finally, each process is composed by a set of practices and tips for achieving the process goal.

Figure 1 shows the 3 maturity levels (initial, people managed, and competency managed) and their processes that have been defined in the Cybersecurity maturity Model.

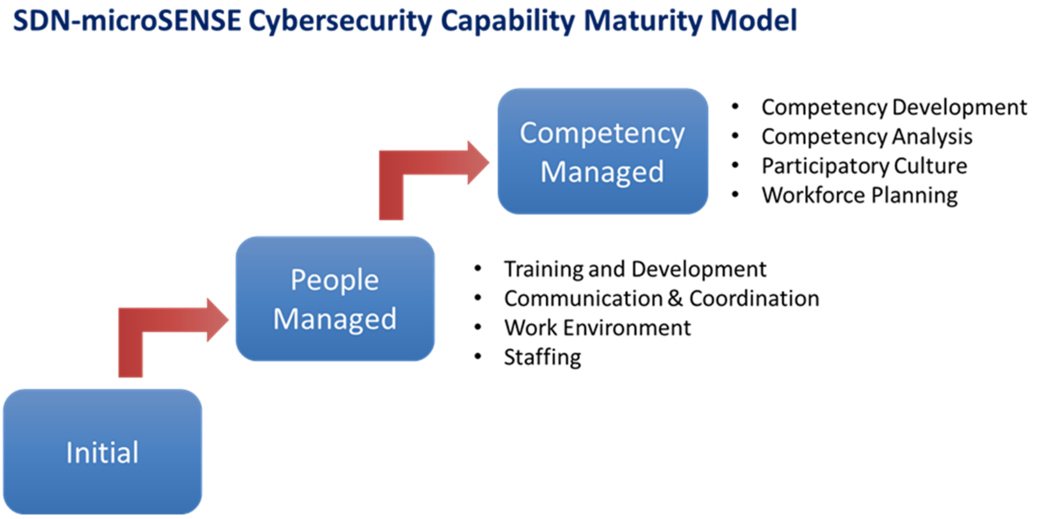


Figure 1. Levels and process of the SDN-microSENSE Cybersecurity Maturity Model

Cybersecurity Competency Framework

A competency model is a framework that defines a set of knowledge, skill and abilities required to perform a specific job in a company. The continuous digitisation of the energy sector is forcing the workforce to acquire cybersecurity knowledge and skills to avoid unconscious errors, reduce external threats, and be able to face adverse events (attacks and incidents) or system failures. The Cybersecurity Competency Framework focusses on specific cybersecurity competences (knowledge, skills and abilities) that must be adopted by each person according to its working role.

A total set of 16 user roles have been defined in the model like executive manager, security administrator, system operator, engineer, OT manager, installer or IT user. Each role includes information about its activity, location, managed assets, possible threats and cybersecurity competences (knowledge, skills and abilities).

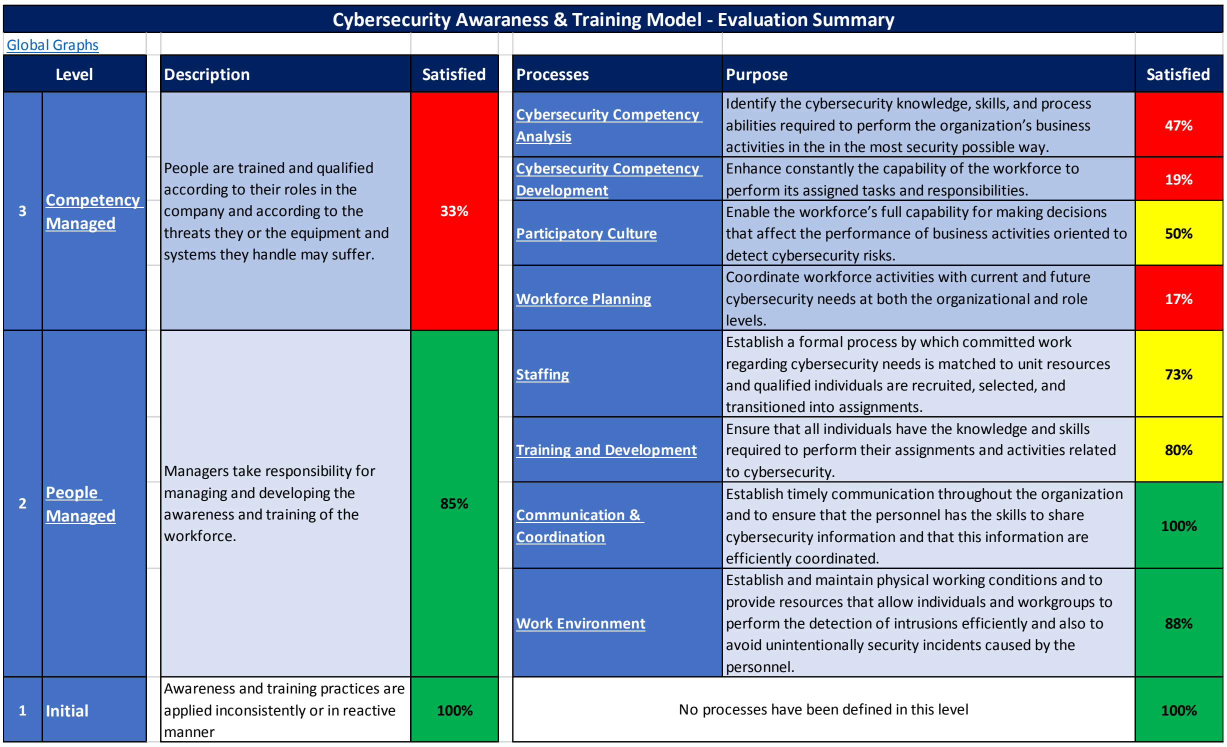
Evaluation tool.

The Evaluation Tool allows a company to measure the maturity level reached in the institutionalisation and deployment of training processes defined in the Cybersecurity Maturity Model. Once the user has entered information about the practices deployed in the company, the tool will give information about the level of maturity reached by the company.

The tool, developed in EXCEL, contains the following elements:

- Cover form. It provides general information of the tool: name, version, brief description,
- Evaluation summary form.
- Level 2 (people managed) results presentation form.
- Level 3 (competency managed) results presentation form.
- Processes assessment form.

Figure 2 shows the summary form of the evaluation tool which provides information about the degree of deployment of the different maturity processes.



Cybersecurity Awareness & Training Model - Evaluation Summary

Global Graphs

Level		Description	Satisfied	Processes	Purpose	Satisfied
3	Competency Managed	People are trained and qualified according to their roles in the company and according to the threats they or the equipment and systems they handle may suffer.	33%	Cybersecurity Competency Analysis	Identify the cybersecurity knowledge, skills, and process abilities required to perform the organization's business activities in the in the most security possible way.	47%
				Cybersecurity Competency Development	Enhance constantly the capability of the workforce to perform its assigned tasks and responsibilities.	19%
				Participatory Culture	Enable the workforce's full capability for making decisions that affect the performance of business activities oriented to detect cybersecurity risks.	50%
				Workforce Planning	Coordinate workforce activities with current and future cybersecurity needs at both the organizational and role levels.	17%
2	People Managed	Managers take responsibility for managing and developing the awareness and training of the workforce.	85%	Staffing	Establish a formal process by which committed work regarding cybersecurity needs is matched to unit resources and qualified individuals are recruited, selected, and transitioned into assignments.	73%
				Training and Development	Ensure that all individuals have the knowledge and skills required to perform their assignments and activities related to cybersecurity.	80%
				Communication & Coordination	Establish timely communication throughout the organization and to ensure that the personnel has the skills to share cybersecurity information and that this information are efficiently coordinated.	100%
				Work Environment	Establish and maintain physical working conditions and to provide resources that allow individuals and workgroups to perform the detection of intrusions efficiently and also to avoid unintentionally security incidents caused by the personnel.	88%
1	Initial	Awareness and training practices are applied inconsistently or in reactive manner	100%	No processes have been defined in this level		100%

Figure 2. Evaluation tool. Evaluation summary form.

1 Introduction

The standard IEC-62443-2-1 considers "*Security awareness for all personnel is an essential tool for reducing cyber security risks. Knowledgeable and vigilant staff are one of the most important lines of defense in securing a system. It is therefore important for all personnel to understand the importance of security in maintaining the safe operation of the system. All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering*" [1].

In the same line, the American standard NERC CIP, elaborated by the North American Electric Reliability Corporation[1] gives personnel training an especial relevance. Part CIP-004 of the standard defines a set of requirements with the objective to "*minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems."* [2].

The European Agency of Cybersecurity, ENISA, in its report "Threat Landscape and Good Practice Guide for Smart Home and Converged Media", identifies Employees as one of the threat agents in a smart grid. By employees the report defines "*staff, contractors, operational staff or security guards of a company. They can have access to company's resources, and they are considered as both non-hostile threats agents (i.e. distracted employees) as well as hostile ones (i.e. disgruntled employees)"* [3].

On the other hand, a concern exists in the energy companies about the low level of training in their staff regarding cybersecurity, what it is considered a real risk in the security of the company and the infrastructures they operate. Companies are aware that they need to improve the knowledge of their employees, especially those that are operating the most critical assets of the company.

With this in mind, Task 3.4 of the SDN-microSENSE project, addresses this challenge. In this task a methodology and an evaluation tool have been developed that help energy companies to improve and assess the readiness and awareness level of both energy-related personnel, EPES directors and managers as well as organizational procedures, processes and controls.

1.1 Purpose of the document

This document contains the work done in Task 3.4 of the SDN-microSENSE project, *Energy-related Personnel & Processes Readiness Evaluation,* where a Cybersecurity Awareness and Training Model and Evaluation Tool have been developed. The model provides the information needed by an energy company to institutionalise a set of processes to manage the cybersecurity awareness and training of its personnel. The evaluation tool helps to assess the level of maturity reached by the company in the deployment of the processes defined in the model.

[1] North America Reliability Corporation. https://www.nerc.com/

The Cybersecurity Awareness and Training Model contains the following elements:

- An EPES User Roles catalogue. This catalogue, that it is aligned with the roles presented in D2.2 document, contains a description of sixteen different user roles that can exist in an energy company. For each role the following information is provided: role description, location, smart grid assets that are managed, controlled or operated and the threats that can affect the assets.
- A Cybersecurity Maturity Model of the company. This model contains a set of processes and the corresponding practices that must be institutionalised to successfully manage cybersecurity training in the company.
- A Cybersecurity Competency Framework. This framework contains an exhaustive list of cybersecurity knowledge, skills and abilities that are required by each role in an energy company.
- An Evaluation Tool. The tool is developed in EXCEL and helps the company to assess its maturity level in the deployment of the cybersecurity training process.

1.2 Methodology

Figure 3 shows the methodology followed to develop the SDN-microSENSE Cybersecurity Awareness and Training Evaluation Tool. The following steps are included:

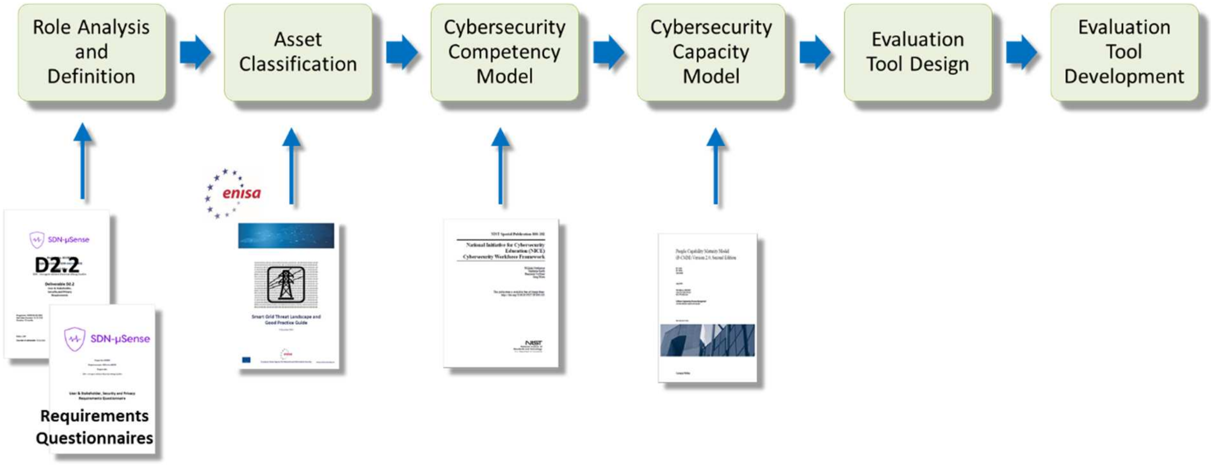

Role Analysis and Definition
Asset Classification
Cybersecurity Competency Model
Cybersecurity Capacity Model
Evaluation Tool Design
Evaluation Tool Development
SDN-μSense
D2.2
enisa
SDN-μSense
Requirements Questionnaires

Figure 3. Methodology followed to elaborate the SDN-microSENSE Cybersecurity Awareness and Training Evaluation Tool

1. Role Analysis and Definition. In this first task of the process, the catalogue of the user roles in an energy company has been done. For this analysis, deliverable D2.2 and the set of *User & Stakeholder, Security and Privacy Requirements Questionnaires* elaborated by the project partners have been used as main inputs.
2. Asset Classification. In this task, it has been identified which smart grid assets can be assigned to each user role. As input the ENISA's report "Threat Landscape and Good Practice Guide for Smart Home and Converged Media" has been used [3].

3. Cybersecurity Competency Model. In this task, we have selected the cybersecurity competences (knowledge, skills and abilities) that are required for each user role, from the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [4]. NICE Framework has been elaborated by NIST, the National Institute of Standards and Technology[2].
4. Cybersecurity Capacity Model. In this task, the maturity model to manage the cybersecurity training process in a company in a successful way has been defined. For this task People Capability Maturity Model (P-CMM) [5], elaborated by the Software Engineering Institute has been used as a reference.
5. Evaluation Tool Design. In this task a design of an EXCEL tool to help the company evaluate its maturity level regarding cybersecurity training has been done.
6. Evaluation Tool Development. Finally, the evaluation tool designed in the previous task has been developed.

1.3 Structure of the document

Deliverable 3.4 is divided into the following sections:

- Section 1 is the introductory part of the report and gives the objective and the methodology used to elaborate the document.
- Section 2 provides a general vision of the awareness and training evaluation methodology. It analyses cybersecurity standards that include requirements for awareness and training, existing capacity methodologies that measure the way company manage people, and competence frameworks that defines the knowledges and skill of the people to perform specific functions in the company.
- Section 3 provides the user roles classification in an energy company and the assets and threats that cab assigned to each user role.
- Section 4 presents the evaluation process of the maturity of an energy company regarding the cybersecurity awareness and training of its personnel. It includes a revision of existing maturity models and the description of the SDN-microSENSE Maturity Model.
- Section 5 contains the SDN-microSENSE Cybersecurity Competency Model defined for energy companies.
- Section 6 provides information about the EXCEL Tool that has been developed to support energy company to evaluate the cybersecurity awareness and training process in the company and the competence level acquired by the personnel of the company.
- Annex I provides a detailed description of the SDN-microSENSE User Roles with the assets, the treats associated to these assets and the knowledge required for this role.

[2] National Institute of Standards and Technology. https://www.nist.gov

1.4 Relation to other Work Packages

Figure 4 depicts the relationships of the deliverable to the other Work Packages (WPs).

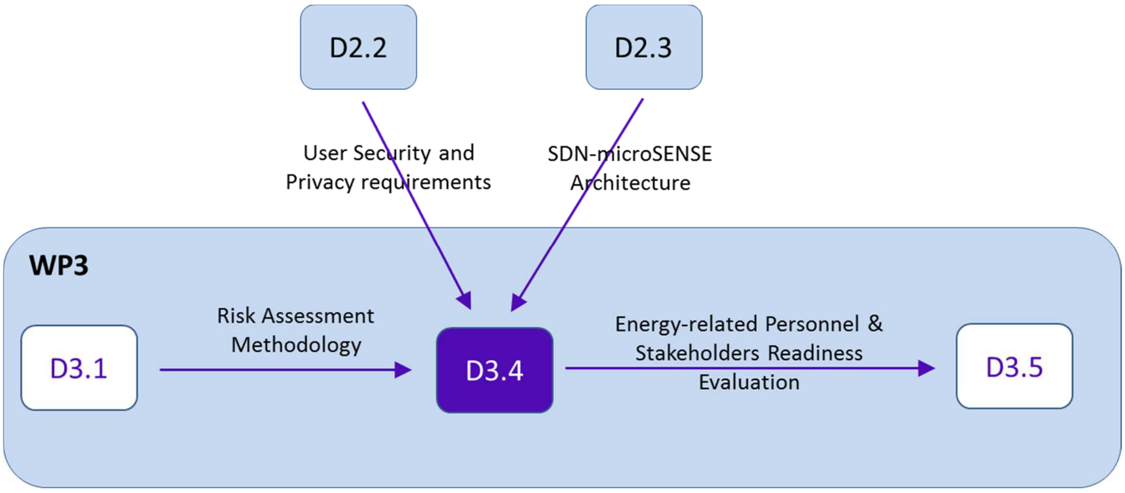

D2.2
D2.3
User Security and Privacy requirements
SDN-microSENSE Architecture
WP3
D3.1
Risk Assessment Methodology
D3.4
Energy-related Personnel & Stakeholders Readiness Evaluation
D3.5

Figure 4. Deliverable D3.4 relationship within the SDN-microSENSE

The main input for D3.4 has been D2.2, "User & Stakeholder, Security and Privacy Requirements" [6]. D2.2 identifies the EPES stakeholders, personnel User Roles in EPES organizations and External EPES actors. This initial list has been augmented with other roles that were also identified by the project partners in the "*User & Stakeholder, Security and Privacy Requirements Questionnaires*" elaborated during the task T2.2 of the project. Section 3.1 provides a complete list of user roles that have been considered in this document.

On the other hand, some SDN-microSENSE requirement have been addresses in D3.4. These requirements are listed in Table 1.

Table 1. SDN-microSENSE Requirements relevant to the Energy-related Personnel & Processes Readiness Evaluation.

ID	Description	Priority
OR-GR-01	The Executive Management should organise regular awareness training and certification programs for staff responsible for implementing and maintaining the security of control systems and networks.	High
OR-GR-03	The Executive Management should also ensure the appropriate training and certification programs are accessible also for third party contractors and vendors with access to the system.	High

Generally, the main result of an evaluation process is a report containing the maturity level reached by a company and the practices and processes that have been satisfied by the organization. This information could be used by the risk analysis process as a measure of the risk due to the human factor in the following way: the lower number of practices deployed in a company, the greater the risk related to the human factor.

2 Cybersecurity Awareness and Training Model and Evaluation

2.1 Why we need a Cybersecurity Awareness and Training Model and Evaluation?

The deployment of a methodology regarding personnel training in a company is essential and particularly justified by the following reasons:

- Cybersecurity standards, like IEC 62443 and NERC CIP, include training requirements to the company employees as a way to reduce cybersecurity risks and to be ready to detect and respond to a cyberattack.
- Distractions or unintentional mistakes based on a lack of knowledge can lead to serious incidents.
- The concern that exists in the energy companies about the knowledge level of the workforce required to adopt cybersecurity measures to protect critical infrastructures.

The Cybersecurity Awareness and Training Model and Evaluation contains a set of components that can be used by an EPES company to:

- Define and adopt a set of internal processes that allow the company to acquire a maturity level in the way the cybersecurity training is managed.
- Select which cybersecurity knowledge, skills and abilities are required for the different roles that exists in the company.
- Asses the level of maturity the company has achieved.

2.2 Training Requirements in Cybersecurity Standards

It is important that the model can support companies in complying with certain cybersecurity standards. An exhaustive analysis of the EPES standards has been elaborated in Deliverable 3.1 [7]. In this document only those standards containing requirements for personnel cybersecurity training process have been analysed:

- 2.4.1 IEC 62443-2-1 Staff training and security awareness.
- 2.4.2 NERC CIP-004-06 Cyber Security – Personnel & Training.
- 2.4.3 NISTIR 7628 Guidelines for Smart Grid Cybersecurity: SG.AT – Awareness and Training.

2.2.1 IEC 62443-2-1 Staff training and security awareness

IEC 62443 [1] is the global standard for the security of Industrial Control System (ICS) networks and supports organizations to reduce both the risk of failure and exposure of ICS networks to cyberthreats. In part 2-1, the standard recommends a company to develop and implement an organisational-wide Cyber Security Management System (CSMS) which includes three processes:

- Risk analysis,
- Addressing risk with the CSMS, and
- Monitoring and improving the CSMS.

It is in the second process where the “Staff training and security awareness” is addressed, as it is shown in the Figure 5. The objective of the Staff training and security awareness process is to *“Provide all personnel (including employees, contract employees and third-party contractors) with the information necessary to identify, review, address and where appropriate, remediate vulnerabilities and threats to IACS and to help ensure their own work practices are using effective countermeasures.”*[3]

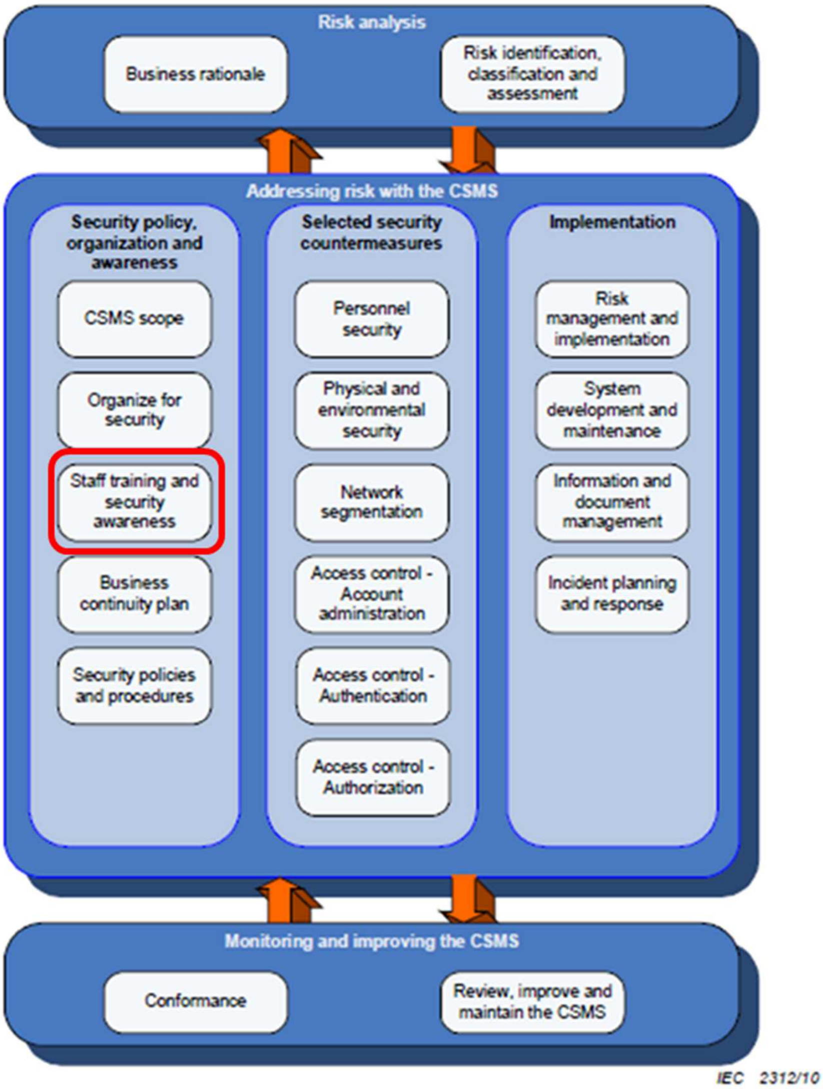

Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control - Account administration
Access control - Authentication
Access control - Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve and maintain the CSMS
IEC 2312/10

Figure 5. IEC 62443-2-1. Cyber Security Management System

Table 2 lists the requirements that have been defined under the Staff Training and Security Awareness.

[3] IEC 62443-2-1. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. 2010.

Table 2. IEC 62443-2-1. Staff Training and Security Awareness Requirements

No	Requirement	Description
R1	Develop a training program	The organization shall design and implement a cyber security training program
R2	Provide procedure and facility training	All personnel (including employees, contract employees, and third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities
R3	Provide training for support personnel	All personnel that perform risk management, IACS engineering, system administration/ maintenance and other tasks that impact the CSMS should be trained on the security objectives and industrial operations for these tasks.
R4	Validate the training program	The training program should be validated on an on-going basis to ensure that personnel understand the security program and that they are receiving the proper training.
R5	Revise the training program over time	The cyber security training program shall be revised, as necessary, to account for new or changing threats and vulnerabilities.
R6	Maintain employee training records	Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis.

2.2.2 NERC CIP-004-06 Cyber Security – Personnel & Training

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid[4]. NERC develops and enforces Reliability Standards. One of these standards is the NERC CIP (for Critical Infrastructure Protection) plan, which is a set of security requirements designed for the assets installed in the Smart Grid with the objective of guaranteeing its security. The current version of the standard is version 6 published in June 2014.

NERC CIP is composed by 14 documents specifying the requirements for different aspects of the infrastructure: asset categorisation, security management control, personnel & training, incident reporting, recovery plans, configuration change management, etc. The document NERC CIP-004 includes a set of requirements “to minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.” [2].

Table 3 lists CIP-004 requirements for personnel and training.

[4] https://www.nerc.com/AboutNERC/Pages/default.aspx

Table 3. NERC CIP-004 Personnel & Training Requirements

No	Requirement Description
R1	**Security Awareness Program** This requirement ensures that people who have authorized electronic or authorized unescorted physical access to BES Cyber Assets maintain awareness of the Responsible Entity's security practices.
R1.1	At least once each calendar quarter, reinforces cyber security practices.
R2	**Cyber Security Training Program** This requirement ensures that the training program covers the proper policies, access controls, and procedures to protect BES Cyber Systems and are trained before access is authorized.
R2.1	Training content on: ▪ Cyber security policies; ▪ Physical access controls; ▪ Electronic access controls; ▪ The visitor control program; ▪ Handling of BES Cyber System Information and its storage; ▪ Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; ▪ Recovery plans for BES Cyber Systems; ▪ Response to Cyber Security Incidents; and ▪ Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.
R2.2	Require completion of the training specified in Part 2.1 prior to granting authorized access to applicable Cyber Assets
R2.3	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.
R3	**Personnel Risk Assessment Program** This requirement ensures that individuals have been assessed for risk within the last 7 years.
R3.1	Process to confirm identity.
R3.2	Process to perform a seven-year criminal history records check as part of each personnel risk assessment.
R3.3	Criteria or process to evaluate criminal history records checks for authorizing access.
R3.4	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.
R3.5	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.
R4	**Access Management Program** This requirement ensures that individuals with access to BES Cyber Systems and the physical and electronic locations have been properly authorized for such access.
R4.1	Process to authorize based on need: ▪ Electronic access; ▪ Unescorted physical access into a Physical Security Perimeter; and

No	Requirement Description
	▪ Access to designated storage locations, whether physical or electronic, for BES Cyber System Information
R4.2	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.
R4.3	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.
R4.4	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.
R5	**Access Revocation** This requirement ensures that when an individual no longer requires access to a BES Cyber System to perform his or her assigned functions, that access should be revoked.
R5.1	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action and complete the removals within 24 hours of the termination action.
R5.2	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary
R5.3	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information
R5.4	For termination actions, revoke the individual's non-shared user accounts
R5.5	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action.

In the definition of the SDN-microSENSE Cybersecurity Awareness and Training Model the first three requirements have been considered:

- R1. Security Awareness Program
- R2. Cyber Security Training Program
- R3. Personnel Risk Assessment Program

R4 and R5 requirements address the procedure to grant and revoke access permissions to company personnel or external parties which are not considered in our model.

2.2.3 NISTIR 7628 Guidelines for Smart Grid Cybersecurity. Awareness and Training

The US Smart Grid Interoperability Panel (SIGP) Cybersecurity Working Group published the "NISTIR 7628, Guidelines for Smart Grid Cybersecurity", in 2010 [8] evaluating the security problems of the Smart Grid. Its content proposes guidelines for selecting and modifying cybersecurity requirements, with the aim of guaranteeing the interoperability of the solutions implemented in the system.

The document, in its 3rd chapter provides a detailed description of 19 security recommended requirements including 7 requirements for Smart Grid Awareness and Training (SG.AT) which address the following objective:

"Smart grid information system security awareness is a critical part of smart grid information system incident prevention. Implementing a smart grid information system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities" [8].

Smart Grid Awareness and Training requirements are listed in Table 4.

Table 4. NISTIR 7628 SG.AT – Awareness and Training

Req No	Requirement Description
SG.AT1	Awareness and Training Policy and Procedures. • The organization develops, implements, reviews, and updates on an organization-defined frequency- a documented awareness and training security policy. • Management commitment ensures compliance with the organization's security policy and other regulatory requirements; • The organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations
SG.AT2	Security Awareness. The organization provides basic security awareness briefings to all Smart Grid information system users (including employees, contractors, and third parties) on an organization-defined frequency
SG.AT3	Security Training The organization provides security-related training • Before authorizing access to the Smart Grid information system or performing assigned duties; • When required by Smart Grid information system changes; and • On an organization-defined frequency thereafter.
SG.AT4	Security Awareness and Training Records The organization maintains a record of awareness and training for each user in accordance with the provisions of the organization's training and records retention policy
SG.AT5	Contact with Security Groups and Associations The organization establishes and maintains contact with security groups and associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents
SG.AT6	Security Responsibility Testing

Req No	Requirement Description
	• The organization tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the Smart Grid information system; • The organization maintains a list of security responsibilities for roles that are used to test each user in accordance with the provisions of the organization training policy; and • The security responsibility testing needs to be conducted on an organization-defined frequency and as warranted by technology/procedural changes.
SG.AT7	Planning Process Training The organization includes training in the organization's planning process on the implementation of the Smart Grid information system security plans for employees, contractors, and third parties

2.3 Components of the Cybersecurity Awareness and Training Model and Evaluation

Figure 6 shows the components of the SDN-microSENSE Cybersecurity Awareness and Training Model and Evaluation):

1. An EPES User Roles catalogue. This catalogue contains the description of sixteen User Roles that exist in the Energy Companies like system and power plant operator, substation engineer, OT manager, installer, or security administrator. For each role, the catalogue contains the role description, location, assets that are managed, operated or maintained and common threats associated to the assets.
2. A Cybersecurity Maturity Model. Three maturity levels that define the degree in which the awareness and training processes have been deployed in the company.
3. A Cybersecurity Capacity Framework. Included in the User Role catalogue, containing a complete set of knowledge, skills and abilities to be acquired by the company personnel to face potential cybersecurity problems.
4. An EXCEL Evaluation Tool to assess the degree of maturity achieved by the company. It provides different check lists to validate whether process have been deployed or not and provides statistics and graphs showing the company's level of maturity.

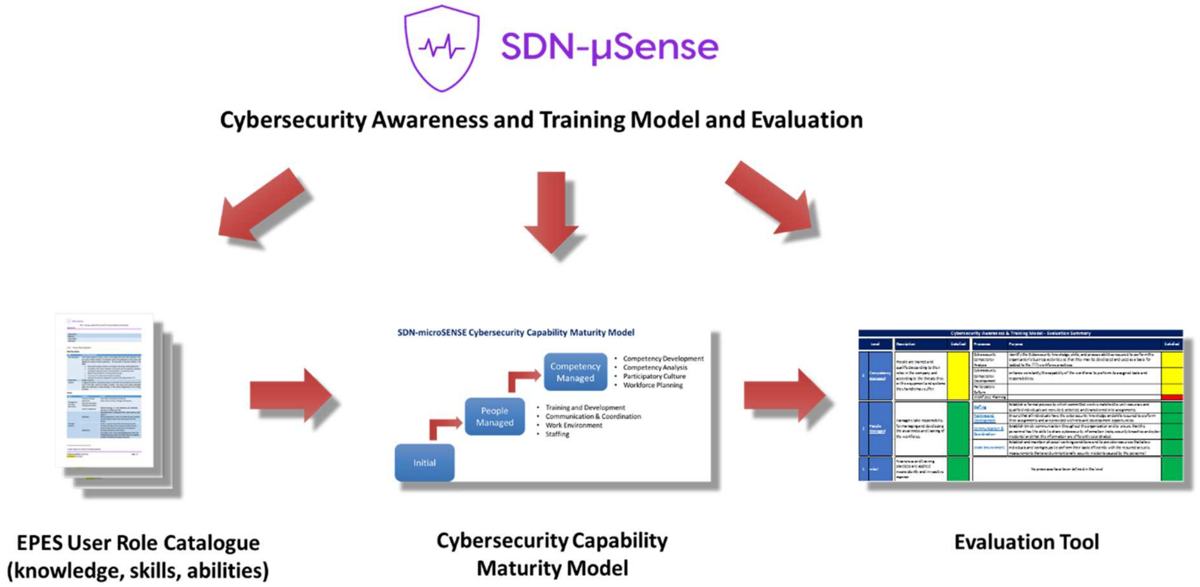


Figure 6. Components of the Cybersecurity Awareness and Training Model and Evaluation

2.4 Target audience

The target audience of the Cybersecurity Awareness and Training Model and Evaluation are the EPES stakeholders. The initial list of stakeholders provided in deliverable D2.2 [6] of the project has been augmented with other roles that were identified by the project partners in the “User & Stakeholder, Security and Privacy Requirements Questionnaires” elaborated during the task T2.2 of the project. A description of the EPES stakeholders and user roles is provided in Section 3.1.

2.5 User Role Catalogue

The user Role Catalogue is a document that contains information about the different activities roles that exists in the company. This catalogue is an important input for the Cybersecurity Awareness and Training Model as will help the company to adapt the training processes to the specific cybersecurity requirements of each activity. The information that includes the User Role Catalogue for each role is the following:

1. Role name
2. Role description
3. Activity of the company (see D2.2)
4. Assets that are managed, controlled or used by the people in the role (see Section 3.3).
5. Threats & Vulnerabilities to which assets may be affected (see Section 3.4).
6. Cybersecurity knowledge that is necessary for the performance of your activity (see Section 5.2).
7. Skills and Abilities that must be acquired (see Section 5.2).

Table 5 shows the template that has been used to gather the user role information. A complete description of the sixteen user roles defined in the SDN-microSENSE project is provided in Annex I.

Table 5. Role Activity Description table

Role		
Role Description		
Stakeholders		
Location		
Assets		
Type	Category	Assets
Information	Asset data	
	Operational	
Managed software	Databases	
	Applications	
Used services	Oriented to the staff	
	Oriented to the network	
Used hardware	Clients	
	Media devices	
	Displays	
	Human interaction	
Infrastructure	Facilities	
Threats & Vulnerabilities		
Type	Category	
Unintentional damage		
Damage/Loss (IT Assets)		
Failures/ Malfunction		
Eavesdropping / Interception		
Nefarious Activity / Abuse		
Cybersecurity Knowledge		
Category	Level	Knowledge
Communication Networks		
Cybersecurity		
Information and Comm Tech		
Information Management		
Laws and Regulations		
Organisational		
Technology Trend		
Skills		
Category	Skill	
Communication Networks		
Cybersecurity		
Information and Comm Tech		
Information Management		
Laws and Regulations		

Organisational	
Abilities	
Category	**Skill**
Communication Networks	
Cybersecurity	
Information and Comm Tech	
Information Management	
Laws and Regulations	
Organisational	

2.6 Integration with the SDN-microSENSE Risk Assessment Framework

As it is shown in Table 5 the User Role Catalogue includes information about the assets, threats and vulnerabilities of the different roles in a company. The best way to obtain this information is through the execution of a Risk Assessment Process.

An EPES Risk Assessment Methodology has been defined in deliverable D3.1 of SDN-microSENSE. It is a risk assessment framework designed to address the various cascading effects that are associated with security incidents occurring in the whole energy chain. The methodology is composed of 7 steps (numbered from 0 to 6) as can be seen in Figure 7:

- Step 0: Scope of the Energy Chain Risk Assessment (ECRA)
- Step 1: Analysis of the EPES
- Step 2: EPES cyber threat analysis
- Step 3: Vulnerability Analysis
- Step 4: Impact Analysis
- Step 5: Risk Assessment
- Step 6: Risk mitigation: Selection of security controls

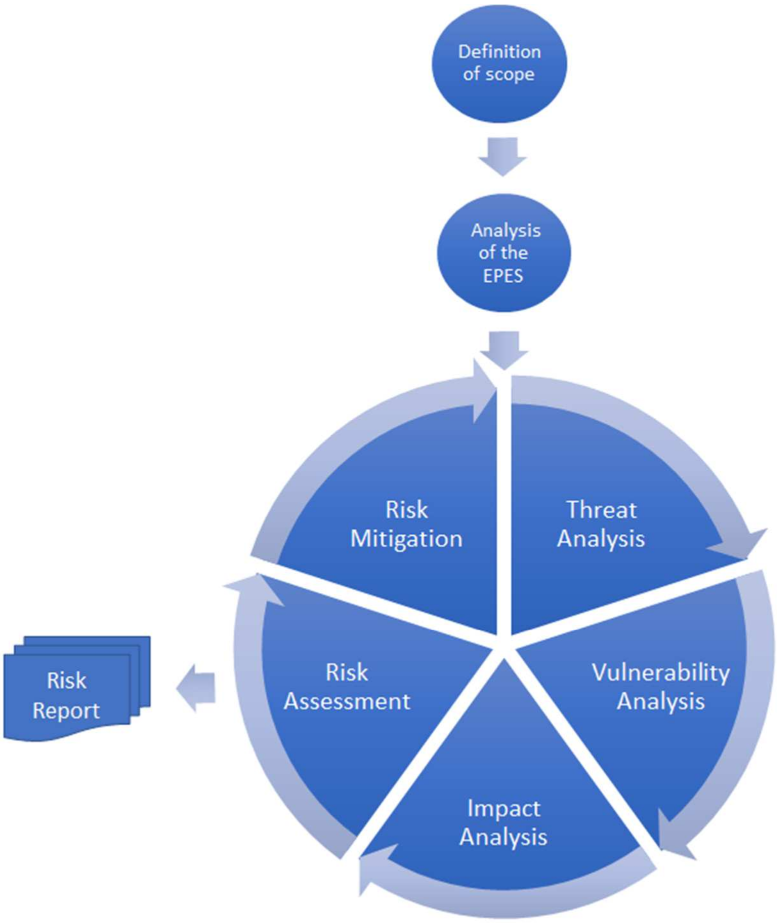
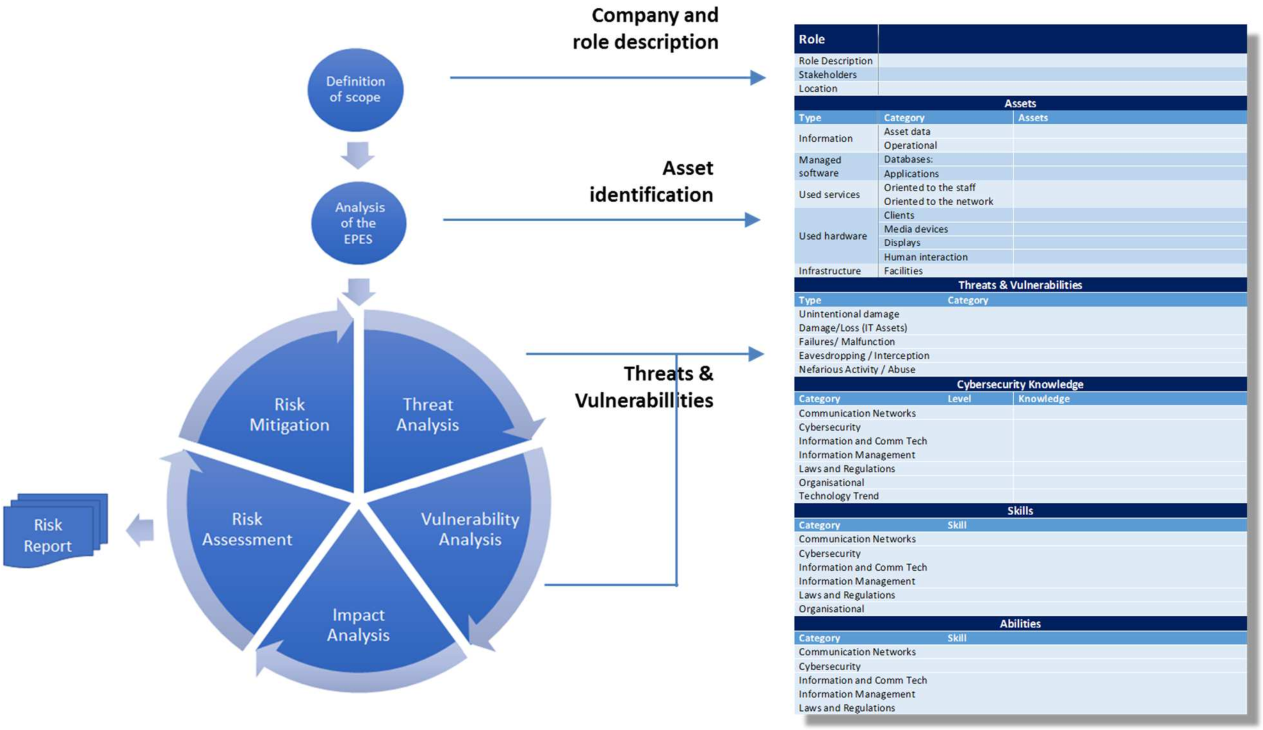


Figure 7. Energy Chain Risk Assessment basic steps

A company can use the results of several steps of the methodology to obtain the information needed to include in the User Role Catalogue. For example, the result of step 1: Analysis of the EPES, will provide the information about which assets are critical in each user role, and steps 2 y 3 threat and vulnerability analysis will generate the input of the Threat and Vulnerability sections in the User Role Catalogue. This integration of the Risk Assessment Methodology and the Cybersecurity Awareness and Training Model can be seen in Figure 8.

Finally, the results of the Risk Analysis can provide, by its own, relevant information to be transmitted to the company personnel during the awareness and training process. Finally, as explained also in Deliverable 3.1, the results of the personnel evaluation can be used for the calculation of the overall Risk Assessment results.



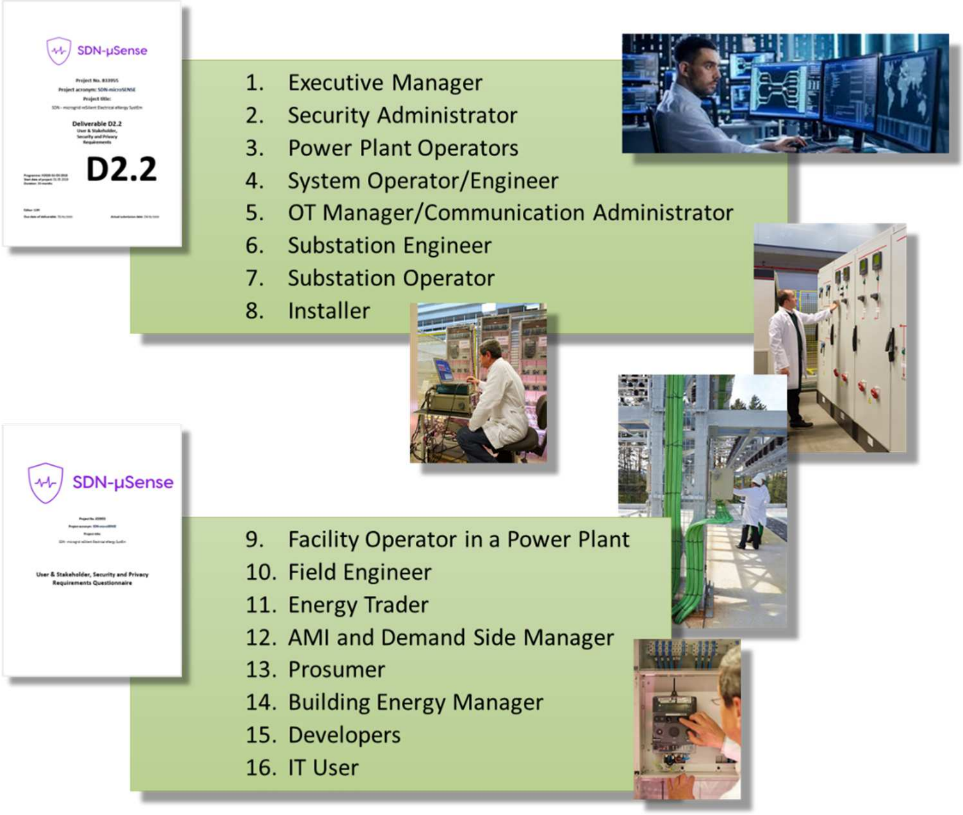
Role		
Role Description		
Stakeholders		
Location		
Assets		
Type	Category	Assets
Information	Asset data	
	Operational	
Managed software	Databases:	
	Applications	
Used services	Oriented to the staff	
	Oriented to the network	
Used hardware	Clients	
	Media devices	
	Displays	
	Human interaction	
Infrastructure	Facilities	
Threats & Vulnerabilities		
Type	Category	
Unintentional damage		
Damage/Loss (IT Assets)		
Failures/ Malfunction		
Eavesdropping / Interception		
Nefarious Activity / Abuse		
Cybersecurity Knowledge		
Category	Level	Knowledge
Communication Networks		
Cybersecurity		
Information and Comm Tech		
Information Management		
Laws and Regulations		
Organisational		
Technology Trend		
Skills		
Category	Skill	
Communication Networks		
Cybersecurity		
Information and Comm Tech		
Information Management		
Laws and Regulations		
Organisational		
Abilities		
Category	Skill	
Communication Networks		
Cybersecurity		
Information and Comm Tech		
Information Management		
Laws and Regulations		

Figure 8. Integration of the Risk Assessment Process with the Cybersecurity Awareness and Training Model

3 Activity Roles in an Energy Company

3.1 EPES Stakeholders and Roles

Section 2.3 of Deliverable 2.2 [6] identifies the EPES stakeholders, personnel User Roles in EPES organizations and External EPES actors. This initial list has been augmented with other roles that were also identified by the project partners in the "*User & Stakeholder, Security and Privacy Requirements Questionnaires*" elaborated during the task T2.2 of the project. The result is a list of sixteen different user roles that are shown in Figure 9.


SDN-μSense
Deliverable D2.2
D2.2
SDN-μSense
User & Stakeholder, Security and Privacy Requirements Questionnaire

1. Executive Manager
2. Security Administrator
3. Power Plant Operators
4. System Operator/Engineer
5. OT Manager/Communication Administrator
6. Substation Engineer
7. Substation Operator
8. Installer
9. Facility Operator in a Power Plant
10. Field Engineer
11. Energy Trader
12. AMI and Demand Side Manager
13. Prosumer
14. Building Energy Manager
15. Developers
16. IT User

Figure 9. List of Activity Roles

More specifically:

- **Executive Manager**: responsible for defining, executing, supervising and updating the operational plan of the organisation including cybersecurity.
- **Security Administrator:** responsible for installing, managing and troubleshooting the organisation's security mechanisms. The security administrator undertakes to ensure the proper operation of the organisation in terms of the security aspect and is also in charge of assuring the readiness and awareness level of all the personnel.

- **Power Plant Operators**: Power plant operators monitor, control, and configure the power plant operation. They use control boards (SCADA[5]) to distribute power from generators among loads and regulate the output of several generators. These systems are the main targets of attack by hackers, since they would allow them to modify and interrupt the physical process of power generation. Special attention should be paid to take any action that allows an intruder to install anything on computers that are connected to this system and to identify any suspicious activity that may mean a threat for the system.
- **System Operator/Engineer**: Engineers/system operators manage the power grid from a set of computer consoles within a control centre. This way, the reliable delivery of electricity to consumers, businesses and industry is ensured. System operators interact with the field staff, general personnel, substation personnel and other system operators within their own utility and/or other utilities. From the cybersecurity point of view his/her responsibilities are similar as in the case of the Power Plant Operators: to avoid taking any action that allows an intruder to install anything in any computer connected to the SCADA and identify any suspicious action or abnormal behaviour of the grid.
- **Operational Technology Manager/Communication Administrator**: An operational technology manager/communication administrator is responsible for monitoring and controlling the operational characteristics of the industrial equipment and the maintenance of the communication channels. This role also involves performing risk assessment regularly in line with the information policies, standards and guidelines.
- **Substation Engineer**: Substation engineers create the design plans of the transmission and distribution substations. Substation engineer should consider cybersecurity aspects during the design phase, probably in collaboration of the OT Manager/Communication Administrator.
- **Substation Operator**: Substation operators monitor and control the operation of transmission or distribution substations. From the cybersecurity point of view their responsibilities are similar at the ones of the Power Plan Operators.
- **Installer (Technical Staff)**: Installer oversees the installation and maintenance of the electrical and electronic devices. Installer should guarantee the security of the whole system, after any installation and maintenance process. He/she should be able to detect any situation that could indicate that there has been an intrusion into the system.
- **Facility Operator in a Power Plant**: Facility operators operate the electrical equipment of the power plant. Like substation operator but in a power plant.
- **Field Engineer**: Field engineers maintain and protect the physical infrastructure of the power plant. Similar that Substation engineer.
- **Energy Trader**. Energy traders trade of energy between cooperating parties and cooperate with the System Operator to achieve the desired status. This role could be done by the system operator in a TSO.
- **AMI and Demand Side Manager**. AMI managers gather real-time meter readings and managing load control switching mechanisms.
- **Prosumer**: Prosumers generate, store and consume renewable energy in its environment.
- **Building Energy Manager**: Providing energy-related services to end-users.

[5] SCADA. Supervisory Control And Data Acquisition.

- **Developers**: They develop and provide hardware and software components and solutions.
- **IT User**: people from administrative departments supporting the operational roles.

Table 6 shows the different activity roles identified in the different energy companies.

Table 6. User Roles in an EPES company

Stakeholder User Role	Role description	Fossil Fuel Energy Producer	Renewable Energy Producer	TSO	DSO	Energy Services providers	Prosumer	Manufacturer
Executive Manager	Defining, executing, supervising and updating the operational plan of the organisation	✓	✓	✓	✓	✓	✓	✓
Security Administrator	Installing, managing and troubleshooting the organisation's security	✓	✓	✓	✓	✓	✓	✓
Power Plant Operator	Monitoring, controlling and configuring the power plant operation	✓	✓					
Facility Operator (Power Plant)	Operating the electrical equipment of the power plant	✓	✓					
Field Engineer	Maintaining and protecting the infrastructure	✓	✓					
System Operator / Engineer	Managing the power grid from a set of computer consoles within a control centre			✓	✓			
Energy Trader	Trading of energy between cooperating parties. Cooperating with the System Operator to achieve the desired status			✓				
AMI and Demand Side Manager	Gathering real-time meter readings and managing load control switching mechanisms				✓	✓	✓	
Operational Tech Manager / Communication Administrator	Monitoring and controlling the operational characteristics of the industrial equipment	✓	✓	✓	✓	✓	✓	✓
Substation Engineer	Creating the design plans of the transmission or distribution substations			✓	✓			

Stakeholder User Role	Role description	Fossil Fuel Energy Producer	Renewable Energy Producer	TSO	DSO	Energy Services providers	Prosumer	Manufacturer
Substation Operator	Monitoring and controlling the operation of transmission or distribution substations			✓	✓			
Installer	Installing and maintaining of the electrical and electronic devices	✓	✓	✓	✓	✓	✓	✓
Prosumer	Generating, storing and consuming renewable energy in its environment						✓	
Building Energy Manager	Providing energy-related services to end-users					✓		
Developer	Developing and providing hardware and software components and solutions							✓
IT User	Supporting the operational roles	✓	✓	✓	✓	✓	✓	✓

3.2 Matching User Roles with Smart Grid Architecture Model (SGAM)

The Smart Grid Architecture Model (SGAM)[6] is a reference model to analyse and visualize smart grid use cases in respect to interoperability, domains and zones. As it is shown in Figure 10, SGAM consists of five consistent layers representing business objectives and processes, functions, information models, communication protocols and components. These five layers represent an abstract version of the interoperability categories introduced in the Reference Architecture working group report. A brief description of the each SGAM layer is provided in Table 7.

The intention of this model is to allow the presentation of the current state of implementations in the electrical grid, but furthermore to present the evolution to future smart grid scenarios by supporting the principles universality, localization, consistency, flexibility and interoperability [9].

[6] The Smart Grid Architecture Model (SGAM) was created in the M/490 mandate of the European Commission (EC) to the European standardization bodies CEN (Comité Européen de Normalisation), CENELEC (European Committee for Electrotechnical Standardization), and ETSI (European Telecommunications Standards Institute) with the focus on finding existing technical standards applicable to Smart Grids as well as identifying gaps in state-of-the-art and standardization.

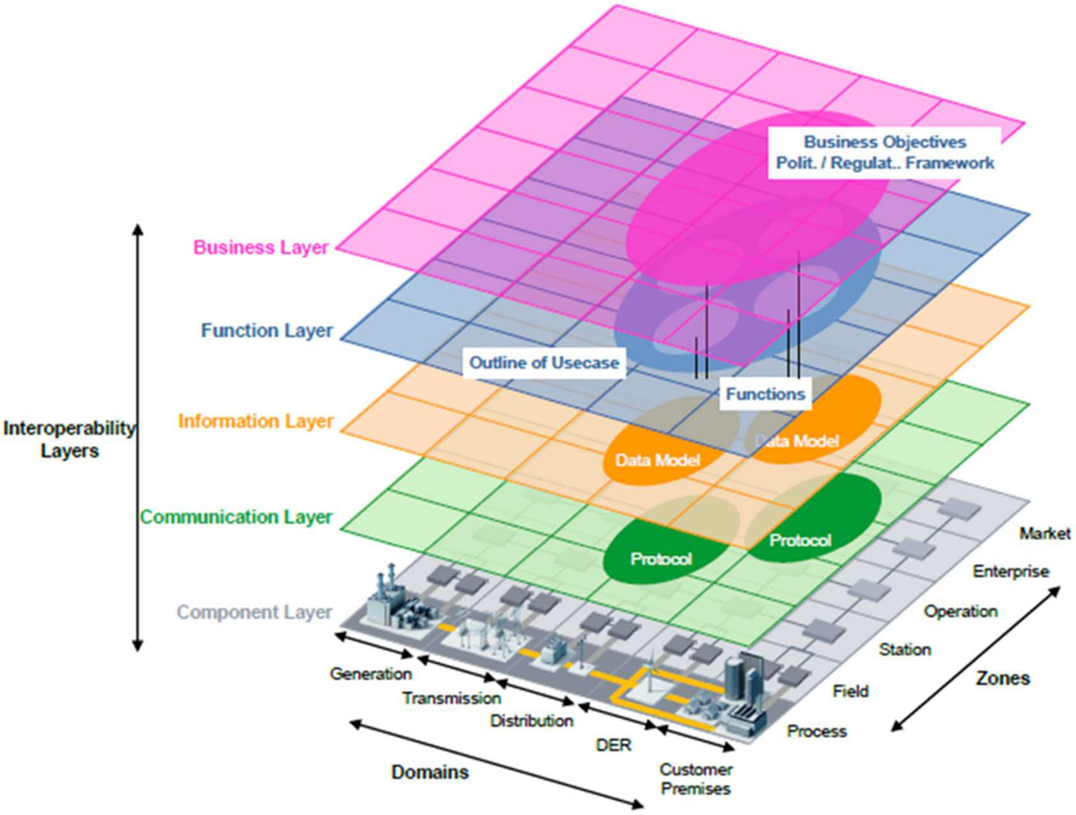


Figure 10. SGAM Framework.

Table 7. SGAM Layers

Layer	Description
Business	Represents business cases which describe and justify a perceived business need
Function	Represents use cases including logical functions or services independent from physical implementations
Information	Represents information objects or data models required to fulfil functions and to be exchanged by communication
Communication	Represents protocols and mechanisms for the exchange of information between components
Component	Represents physical components which host functions, information and communication means

SGAM Domains and Zones

Each layer covers the smart grid plane, shown in Figure 11, is spanned by SGAM domains and zones. Zones represent the hierarchical levels of power system management: Process, Field, Station, Operation, Enterprise and Market. Domains cover the complete electrical energy conversion chain:

Bulk Generation, Transmission, Distribution, DER and Customers Premises [9]. Table 8 provides a brief description of SGAM domains, while SGAM zones are described in Table 9.

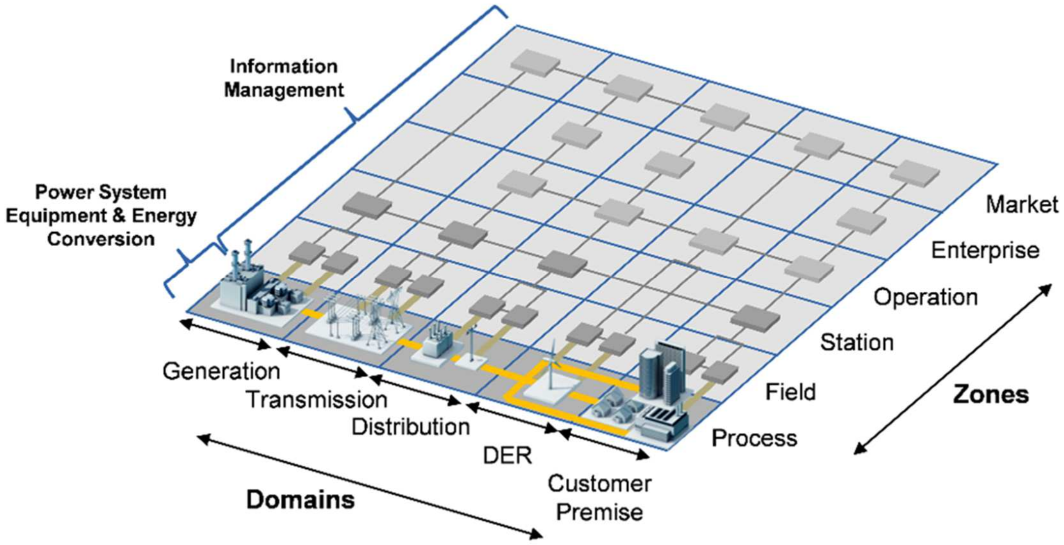


Figure 11. Smart Grid Plane. Domains and hierarchical zones

Table 8. SGAM Domains

Domains	Description
Bulk Generation	Representing generation of electrical energy in bulk quantities, such as by fossil, nuclear and hydro power plants, off-shore wind farms, large scale photovoltaic (PV) power– typically connected to the transmission system
Transmission	Representing the infrastructure and organization which transports electricity over long distances
Distribution	Representing the infrastructure and organization which distributes electricity to customers
DER	Representing distributed electrical resources, directly connected to the public distribution grid, applying small-scale power generation technologies (typically in the range of 3 kW to 10.000 kW). These distributed electrical resources can be directly controlled by DSO
Customer Premises	Hosting of both end users and producers of electricity. The premises include industrial, commercial and home facilities (e.g. chemical plants, airports, harbours, shopping centres, homes). Electricity generation in form of photovoltaic generation, EV storage, batteries or micro turbines is also hosted.

Table 9. SGAM Zones

Zone	Description
Process	Including both - primary equipment of the power system (e.g. generators, transformers, circuit breakers, overhead lines, cables, electrical loads) - as well as physical energy conversion (e.g., electricity, solar, heat, water, wind).

Field	Including equipment to protect, control and monitor the process of the power system, e.g. protection relays, bay controller, any kind of intelligent electronic devices which acquire and use process data from the power system.
Station	Representing the aggregation level for fields, e.g. for data concentration or substation automation.
Operation	Hosting power system control operation in the respective domain, e.g. distribution management systems (DMS), energy management systems (EMS) in generation and transmission systems, microgrid management systems, virtual power plant management systems (aggregating several DER), electric vehicle (EV) fleet charging management systems.
Enterprise	Includes commercial and organizational processes, services and infrastructures for enterprises, e.g. asset management, staff training, customer relation management, billing and procurement.
Market	Reflecting the market operations possible along the energy conversion chain (e.g., energy trading, mass market, retail market).

Finally, Table 10 shows the matching of the EPES user roles defined in this document in the zones and domains of the SGAM model.

Table 10.Matching User Roles with Smart Grid Architecture Model (SGAM)

Executive Manager	Executive Manager Energy Trader	Executive Manager	Executive Manager	Executive Manager Prosumer	**Market**
Security Administrator IT User	Security Administrator IT User	Security Administrator IT User	Security Administrator IT User	Prosumer	**Enterprise**
Power Plant Operator	System Operator	System Operator AMI and DSM	RES Operator	AMI and Demand Side Manager	**Operation**
Field Engineer Facility Operator	Substation Engineer Substation Operator	Substation Engineer Substation Operator	Field Engineer Facility Operator	Building Energy Manager Prosumer	**Station**
OT Manager Installer	OT Manager Installer	OT Manager Installer	OT Manager Installer	OT Manager Installer	**Field**
Installer	Installer	Installer	Installer	Installer	**Process**
Generation	**Transmission**	**Distribution**	**DER**	**Customer Premise**	

3.3 Smart Grid Assets

According the Risk Assessment Framework, defined in Deliverable 3.1, a decomposition of the cyber assets of the infrastructure managed by the company has to be done in step 1 of the Risk Assessment Methodology.

An asset is defined in Deliverable 3.1 as "*anything that is considered to be of value. Generally, an asset may be any physical or virtual entity that needs to be protected. An asset could be the personnel (employees or customers), material, information (e.g. databases or critical data), or intangibles (reputation or intellectual property)*" [7]. In the context of SDN-microSENSE project, assets come from the Smart Grid field (e.g. ICS/SCADA), SDN field and the legacy ICT field.

In the context of the Cybersecurity Awareness and Training Model, assets' analysis is also important to adapt the awareness and training process to the specific user roles defined in the company. Depending on the type of assets (information, hardware devices, communication network components, physical infrastructures, etc.) different knowledge and skills could be required to manage and protect them, and the training process can be adapted to specific asset vulnerabilities.

ENISA[7], the European Union Agency for Cybersecurity, has elaborated a report entitled, "Smart Grid Threat Landscape and Good Practice Guide" [3]. This report provides an exhaustive classification of assets that exist in the Smart Grid, threats to which they are exposed and good practices of the smart grid security measures. In the following subsections we have associated these assets and threats classification with the information provided by project partners during the elaboration of Deliverable 2.2 about user roles that exists in the company, relevant equipment/technologies (e.g. RTUs, PLC, Smart Meters, SCADAs, etc.) used by each user role, type of network (HAN, NAN, WAN, etc.) and their cybersecurity-awareness level. Figure 12, taken from the ENISA's report, shows the assets' classification. This classification to identify the assets that are managed controlled or used in each user roles has been used.

Table 11 provides a classification of the smart grid assets defined in ENISA's report to the user roles identified in the previous section.

[7] ENISA: https://www.enisa.europa.eu/

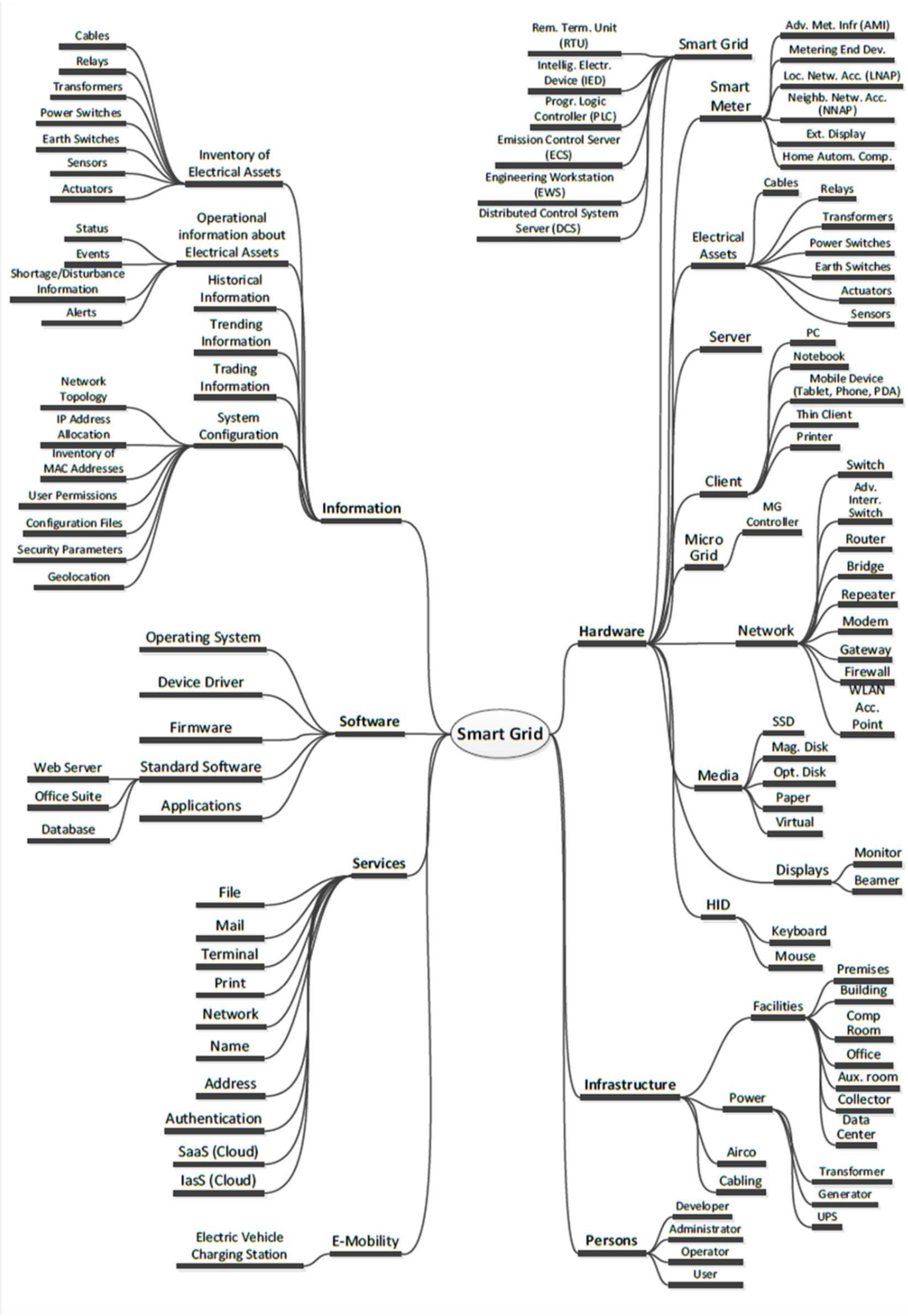


Figure 12. Smart grid assets. Source ENISA[8]

[8] ENISA: https://www.enisa.europa.eu/

Table 11. Association between Company roles and Smart Grid Assets

Asset Type	Description	Category	Asset	Executive Manager	Security Administrator	Power Plant Operator	*Facility Operator (Power Plant)*	*Field Engineer*	System Operator / Engineer	*Energy Trader*	*AMI and Demand Side Manager*	Operational Tech Manager	Substation Engineer	Substation Operator	Installer	***Prosumers***	***Building Energy Manager***	***Developers***	***IT User***
Information	For each information we should consider the level of confidentiality, integrity and availability	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators	☑				☑	☑		☑		☑		☑	☑	☑		☑
		Operational information	Status, alarms, events, shortage, disturbances	☑	☑	☑	☑		☑		☑		☑	☑	☑	☑	☑		☑
		Historical information	Information that must be storage by law	☑	☑					☑	☑					☑	☑		☑
		Trending information	Information about the past that can be used to predict the future	☑	☑	☑			☑	☑	☑					☑	☑		☑
		Trading information	Information with commercial uses	☑						☑	☑					☑	☑		☑
		System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.		☑			☑				☑	☑		☑	☑	☑		☑

Asset Type	Description	Category	Asset	Executive Manager	Security Administrator	Power Plant Operator	*Facility Operator (Power Plant)*	*Field Engineer*	System Operator / Engineer	*Energy Trader*	*AMI and Demand Side Manager*	Operational Tech Manager	Substation Engineer	Substation Operator	Installer	***Prosumers***	***Building Energy Manager***	***Developers***	***IT User***
Software	Consider: origin of software, access to if, location, backup, …	Applications	SCADA, applications to control industrial process.			☑			☑	☑	☑	☑		☑	☑	☑	☑	☑	☑
		Standard Software	Databases, Web servers		☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
		Operating Systems										☑			☑			☑	
		Device Drivers										☑			☑			☑	
		Firmware						☑				☑	☑		☑			☑	
Services	In this case, we must identify which services are needed to do the role	Oriented to the staff	Mail, terminal service, print service, authentication service.	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
		Oriented to the network	File service, network service, name service, address service.		☑							☑	☑	☑	☑		☑	☑	☑
		Cloud services	SaaS, IaaS		☑							☑			☑	☑	☑	☑	☑
Hardware		Smart grid	RTU, IED, PLC, DCS				☑	☑					☑	☑	☑			☑	

Asset Type	Description	Category	Asset	Executive Manager	Security Administrator	Power Plant Operator	Facility Operator (Power Plant)	Field Engineer	System Operator / Engineer	Energy Trader	AMI and Demand Side Manager	Operational Tech Manager	Substation Engineer	Substation Operator	Installer	Prosumers	Building Energy Manager	Developers	IT User
	A main issue talking about hardware is the supply chain	Microgrid	Controllers				☑	☑					☑	☑	☑	☑	☑	☑	
		Smart Meter	End devices, local and neighbourhood network access point, External displays, home automation components, AMI head end								☑					☑	☑	☑	
		Servers	Hardware servers									☑			☑			☑	
		Clients	PC, Notebook, Tablet, mobile-phone, printer, smart appliances (e.g., thermostats, pumps, heaters).	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
		Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point.					☑				☑	☑		☑	☑	☑	☑	

Asset Type	Description	Category	Asset	Executive Manager	Security Administrator	Power Plant Operator	*Facility Operator (Power Plant)*	*Field Engineer*	System Operator / Engineer	*Energy Trader*	*AMI and Demand Side Manager*	Operational Tech Manager	Substation Engineer	Substation Operator	Installer	***Prosumers***	***Building Energy Manager***	***Developers***	***IT User***
		Media devices	Storages (e.g., magnetic, optical, semiconductor, paper)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
		Displays	Monitor, Beamer	☑	☑	☑			☑	☑	☑	☑					☑	☑	☑
		Human interaction	Keyboard, Mouse	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Infrastructure		Facilities	Premises, buildings, Server Room, Office, auxiliary room, collector, Data Centre	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
		Power	Transformer Emergency Generator, UPS					☑				☑		☑		☑	☑		
		Air Conditioning										☑				☑	☑		
		Cabling					☑	☑				☑			☑		☑		
Personnel		User		☑	☑														
		Operator		☑	☑														
		Administrator		☑	☑														
		Developer		☑	☑														

Asset Type	Description	Category	Asset	Executive Manager	Security Administrator	Power Plant Operator	*Facility Operator (Power Plant)*	*Field Engineer*	System Operator / Engineer	*Energy Trader*	*AMI and Demand Side Manager*	Operational Tech Manager	Substation Engineer	Substation Operator	Installer	***Prosumers***	***Building Energy Manager***	***Developers***	***IT User***
eMobility		EV Charging Stations							☑							☑	☑		
		Vehicles														☑			

3.4 Smart Grid Threats

Following with the Risk Assessment Methodology of Deliverable 3.1 [7], the next step is the EPES cyber threat analysis. In this step "*individual cyber threats against the EPES cyber assets are identified based on Energy Chain participants expertise and knowledge, with usage of existing repositories of cyber threats*". This information should be also considered in the Cybersecurity Awareness and Training Model to adapt the training process and the training contents to the specific threats that can be associated to each user role.

A detailed analysis of the threats for EPES has been provided in Deliverable 3.2. Although the "RESTRICTED" classification of Deliverable 3.2 does not allow information disclosure related to Smart Grid Threats, the threat classification that appears in the ENISA's report, Smart Grid Threat Landscape and Good Practice Guide is utilized" [3], and that is shown in Figure 13:

- Physical Attack: bomb, sabotage, vandalism, theft, fraud, unauthorized physical access, etc.
- Unintentional data damage: erroneous use of information and administration of devices, unintentional alteration of data, inadequate design, etc.
- Natural Disasters: fire, flood, pollution, thunder stroke, environmental events, etc.
- Outages: internet outage, loss of support, strike, Energy outage, lack of resources, etc.
- Damage and/or loss of IT Assets: destruction of records, damage by third party, loss of information, etc.
- Failures/ Malfunction: failure or malfunction of devices, disruption of communications or services, etc.
- Eavesdropping, interception of information, hijacking, man in the middle, replay of messages, repudiation of actions, etc.
- Nefarious Activity, abuse, denial of service, malicious code activity, falsification of records, manipulation of hardware/software, unauthorised installation/use of software, unauthorised access to systems, etc.
- Legal: unauthorised use of copyright, violation of law, etc.

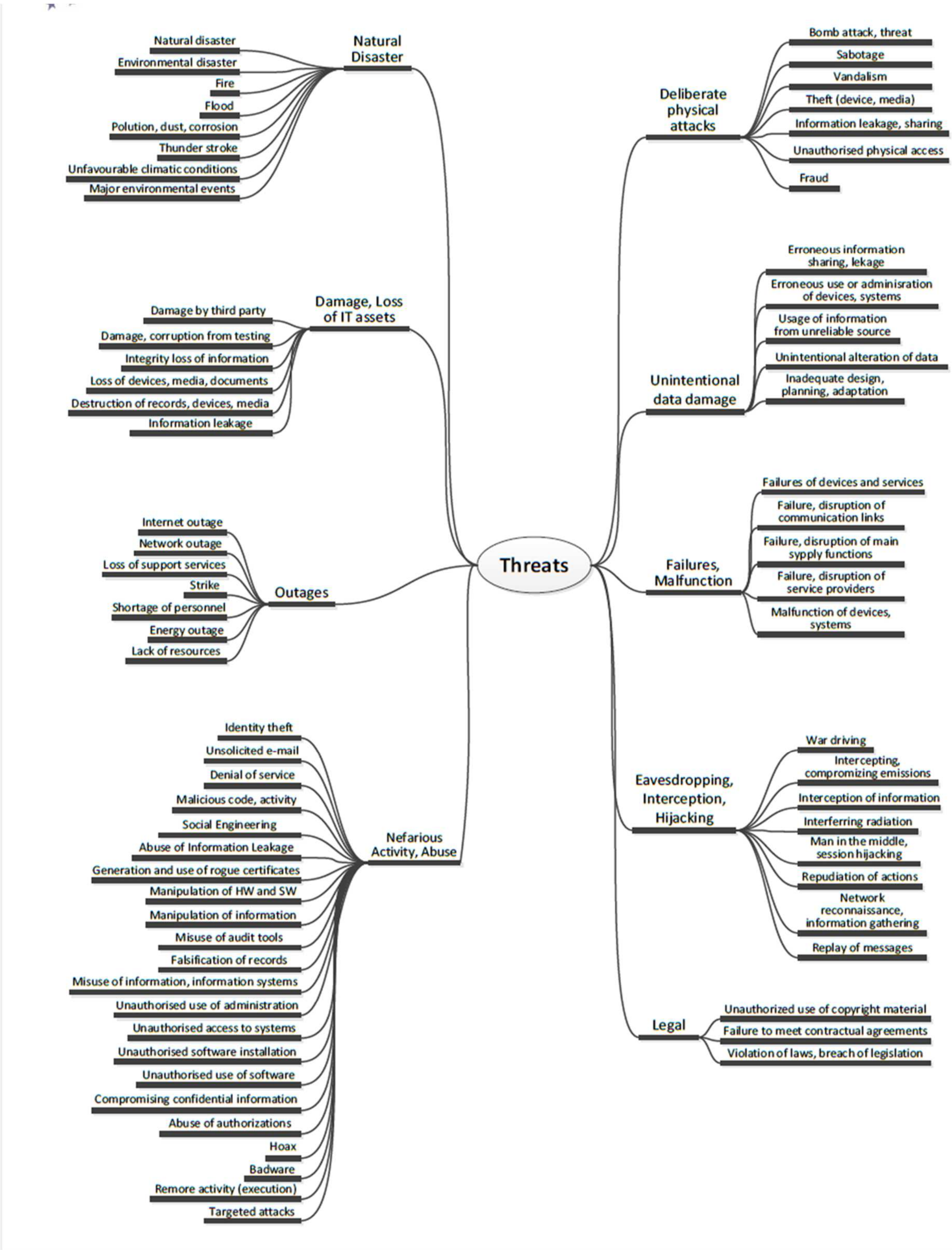

Threats
Natural Disaster
Natural disaster
Environmental disaster
Fire
Flood
Polution, dust, corrosion
Thunder stroke
Unfavourable climatic conditions
Major environmental events
Damage, Loss of IT assets
Damage by third party
Damage, corruption from testing
Integrity loss of information
Loss of devices, media, documents
Destruction of records, devices, media
Information leakage
Outages
Internet outage
Network outage
Loss of support services
Strike
Shortage of personnel
Energy outage
Lack of resources
Nefarious Activity, Abuse
Identity theft
Unsolicited e-mail
Denial of service
Malicious code, activity
Social Engineering
Abuse of Information Leakage
Generation and use of rogue certificates
Manipulation of HW and SW
Manipulation of information
Misuse of audit tools
Falsification of records
Misuse of information, information systems
Unauthorised use of administration
Unauthorised access to systems
Unauthorised software installation
Unauthorised use of software
Compromising confidential information
Abuse of authorizations
Hoax
Badware
Remore activity (execution)
Targeted attacks
Deliberate physical attacks
Bomb attack, threat
Sabotage
Vandalism
Theft (device, media)
Information leakage, sharing
Unauthorised physical access
Fraud
Unintentional data damage
Erroneous information sharing, lekage
Erroneous use or adminisration of devices, systems
Usage of information from unreliable source
Unintentional alteration of data
Inadequate design, planning, adaptation
Failures, Malfunction
Failures of devices and services
Failure, disruption of communication links
Failure, disruption of main sypply functions
Failure, disruption of service providers
Malfunction of devices, systems
Eavesdropping, Interception, Hijacking
War driving
Intercepting, compromizing emissions
Interception of information
Interferring radiation
Man in the middle, session hijacking
Repudiation of actions
Network reconnaissance, information gathering
Replay of messages
Legal
Unauthorized use of copyright material
Failure to meet contractual agreements
Violation of laws, breach of legislation

Figure 13. Smart grid threats. Source ENISA[9]

[9] ENISA: https://www.enisa.europa.eu/

It should be noted that as the focus of the deliverable is the evaluation of personnel and process, the purpose of this section is not to provide an analysis of the threats per se, but highlight the actors, personnel and user roles which can be associated with those threats. For this reason, Table 12 associates threats to Threat Agents and also to Smart Grid Assets.

.

Table 12. Association between threats, threat agents and Smart Grid Assets

Threat Group	Threat	Threat Agents	Assets						
			Information	Software	Services	Hardware	Infrastructure	Persons	e-mobility
Physical Attack	Bomb attack	Terrorist				☑	☑	☑	☑
	Fraud	Employees				☑	☑	☑	☑
	Sabotage	All				☑	☑	☑	☑
	Vandalism	Employees, Terrorists, Rioter				☑	☑	☑	☑
	Theft	All				☑	☑	☑	☑
	Information leakage	All				☑	☑	☑	☑
	Unauthorised physical access	All				☑	☑	☑	☑
	Coercion, extortion or corruption	All							☑
Unintentional damage (accidental)	Information leakage / sharing due to user error	Employees	☑	☑	☑	☑			
	Erroneous use or administration of devices and systems	Employees	☑	☑	☑	☑			
	Using information from an unreliable source	Employees	☑	☑	☑	☑			
	Unintentional change of data in an information system	Employees	☑	☑	☑	☑			
	Inadequate design or lack of adaptation	Employees	☑	☑	☑	☑			
Disaster (natural environmental)	Fire	Natural Disaster				☑	☑	☑	☑
	Flood	Natural Disaster				☑	☑	☑	☑
	Pollution, dust, corrosion	Natural Disaster				☑	☑	☑	☑
	Thunder strake	Natural Disaster				☑	☑	☑	☑

Threat Group	Threat	Threat Agents	Assets						
			Information	Software	Services	Hardware	Infrastructure	Persons	e-mobility
	Water	Natural Disaster				☑	☑	☑	☑
	Unfavourable climatic conditions	Natural Disaster				☑	☑	☑	☑
	Major events in the environment	Natural Disaster				☑	☑	☑	☑
Damage/Loss (IT Assets)	Damage caused by a third party	Third Party	☑	☑	☑	☑			
	Damages resulting from a penetration testing	Third Party	☑	☑	☑				
	Loss of (integrity of) sensitive information	All	☑	☑	☑				
	Loss of device, storage media and documents	All				☑	☑		
	Destruction of records, devices or storage media	All	☑	☑	☑				
	Information leakage	All	☑	☑	☑	☑			
Failures/ Malfunction	Failure of devices or systems	N/A		☑	☑	☑			
	Failure or disruption of communication links	N/A			☑				
	Failure or disruption of main supply	N/A					☑		
	Failure or disruption of service providers	N/A	☑	☑	☑	☑			
	Malfunction of equipment	N/A		☑	☑	☑			
	Insecure Interfaces	N/A		☑	☑	☑			
Outages	Lack of resources	N/A		☑	☑	☑	☑	☑	☑
	Lack of electricity	N/A		☑	☑	☑	☑		☑
	Absence of personnel	N/A						☑	
	Strike	N/A						☑	
	Loss of support services	N/A		☑	☑	☑	☑		☑

Threat Group	Threat	Threat Agents	Assets						
			Information	Software	Services	Hardware	Infrastructure	Persons	e-mobility
	Internet outage	N/A		☑	☑	☑	☑		☑
	Network outage	N/A		☑	☑	☑	☑		☑
Eavesdropping / Interception / Hijacking	War driving				☑				
	Intercepting compromising emissions	All			☑				
	Interception of information	All	☑		☑				
	Interfering radiation	Corporations, Terrorists				☑			
	Replay of messages	Cybercriminals, Employees		☑	☑				
	Network reconnaissance and Information gathering	All	☑		☑			☑	
	Man in the Middle / Session hijacking	All		☑	☑	☑			
	Repudiation of actions	All		☑	☑	☑		☑	
Nefarious Activity / Abuse	Identify theft	All		☑	☑			☑	
	Unsolicited e-mail	Cybercriminals, Hacktivists						☑	
	Denial of Service	Cybercriminals, Hacktivists		☑	☑				
	Malicious code / software / activity	All		☑	☑				
	Social engineering	Cybercriminals, Hacktivists						☑	

Threat Group	Threat	Threat Agents	Assets						
			Information	Software	Services	Hardware	Infrastructure	Persons	e-mobility
	Abuse of information leakage	All		☑	☑	☑		☑	
	Generation and use of rogue certificates	All		☑	☑				
	Manipulation of hardware and software	All		☑	☑	☑			
	Manipulation of information		☑	☑	☑				
	Misuse of audit tools	All	☑	☑					
	Falsification of records		☑	☑					
	Misuse of information	All	☑	☑					
	Unauthorized use of administration of devices and systems	All		☑	☑	☑		☑	
	Unauthorized access to the information system / network	All		☑	☑	☑		☑	
	Unauthorized changes of records	Cybercriminals	☑	☑					
	Unauthorized installation of software	All		☑					
	Unauthorized use of software	All		☑					
	Compromising confidential information (data breaches)	All	☑	☑	☑				
	Abuse of authorisations	All		☑	☑	☑		☑	
	Abuse of person data			☑	☑	☑		☑	
	Hoax	False rumour and/or fake warning		☑	☑	☑		☑	

Threat Group	Threat	Threat Agents	Assets						
			Information	Software	Services	Hardware	Infrastructure	Persons	e-mobility
	Badware	Spyware or deceptive adware	☑	☑	☑				
	Remote activity (execution)	All	☑	☑	☑				
	Targeted attacks	Corporations, Cybercriminals	☑	☑	☑	☑		☑	
Legal	Violation of laws or regulations / Breach of legislation	Corporations, Employees, Cybercriminals	☑	☑				☑	
	Failure to meet contractual requirements	Employees	☑	☑				☑	
	Unauthorized use of copyrighted material	Corporations, Employees, Cybercriminals	☑	☑				☑	

4 Cybersecurity Maturity Model

In the article "Selecting, Using, and creating Maturity Models: a tool for assurance and consulting engagements", J. Rose provides the following definition of a Maturity Model: *"Maturity models establish a systematic basis of measurement for describing the "as is" state of a process. A process's maturity can then be compared to management's expectations or contrasted with the maturity of other similar processes for benchmarking purposes. Insights also can be derived from the model for determining improvement options that help a process to satisfy its intended objectives over time"*[10].

One of the components of the SDN-microSENSE Cybersecurity Awareness and Training Model is the Cybersecurity Maturity Model, in the context of the SDN-microSENSE, the Cybersecurity Maturity Model is defined as a set of processes and practices that have to be defined and deployed in a company to improve the competency level of its personnel in cybersecurity aspects.

SDN-microSENSE Cybersecurity Maturity Model is based on the People CMM [5]. Elaborated by the Software Engineering Institute[11] this model guides organizations in improving their processes for managing and developing their workforce. The People CMM's primary objective is to improve the capability of the workforce, defined as the level of knowledge, skills, and process abilities available for performing an organization's business activities.

Tecnalia is an official partner of CMMI Institute[12] and has an extensive experience related to the CMMI models implementation in industry. Tecnalia has an expert team with proven experience in methods, processes and tools definition, in order to support compliance with these reference models. This is the reason why the use of the People CMM model has been decided as an appropriate reference model for the SDN-microSENSE Capability Maturity Model development.

4.1 People CMMI

The People CMM consists of five maturity levels (Initial, Managed, Defined, Predictable and Optimizing) that establish successive foundations for continuously improving individual competencies, developing effective teams, motivating improved performance, and shaping the workforce an organization needs to accomplish its business plans. Each maturity level of the People CMM, except for the Initial Level, consists of three to seven process areas. Process areas identify the capabilities that must be defined and deployed to achieve a maturity level. They describe the practices that an organization should implement to improve its workforce capability. Figure 14 shows the maturity levels and process areas of each level defined in the People CMM.

[10] J. Rose, "Selecting, Using, and creating Maturity Models: a tool for assurance and consulting engagements", 2017. Available: http://bit.ly/2wyuWPV.

[11]. Software Engineering Institute. https://www.sei.cmu.edu/

[12] https://cmmiinstitute.com/

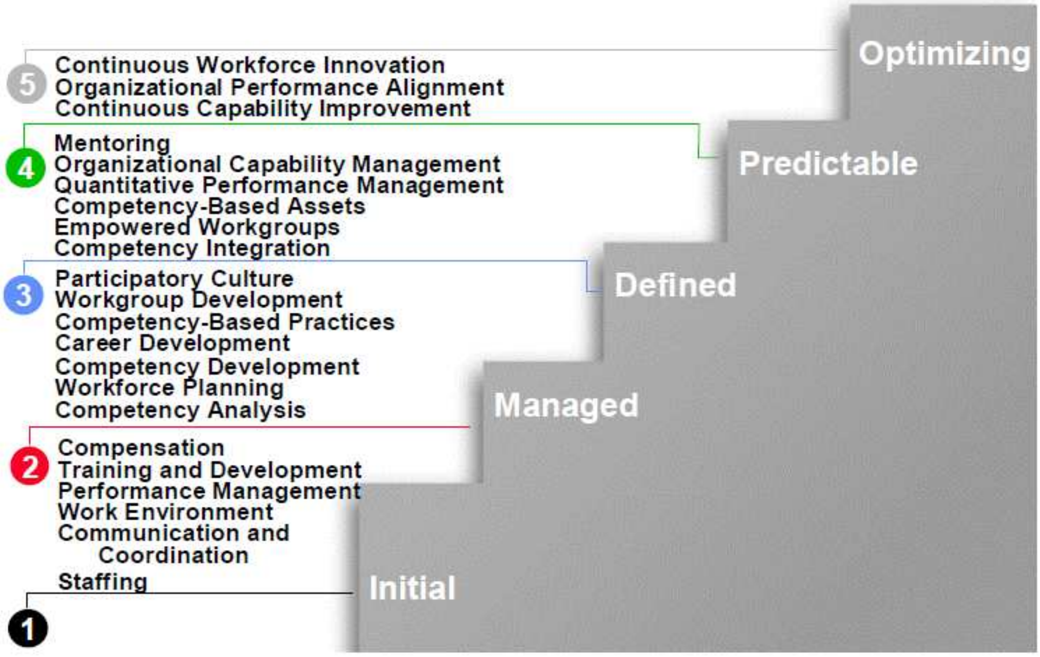


Figure 14. People CMM maturity levels.

Each process area is described through a set of goals, commitments, abilities, practices, measurements and verification. This model provides a good starting point for the definition of a specific cybersecurity maturity model for an energy company.

4.2 SDN-microSENSE Cybersecurity Capability Maturity Model

Cybersecurity training cannot be done in an improvised way, when the company or society has suffered some type of cyber-attack, nor can it be left to the employees themselves. It is necessary to establish a set of procedures that define what skills and knowledge each person should have in the company, depending on their work activity, and how to acquire those skills and knowledge.

The objective of the Cybersecurity Capability Maturity Model is to define best practices in order to improve the capability of an organisation in terms of cybersecurity knowledge, skills, and abilities available for performing cybersecurity activities. It helps organisation in the energy sector to define and implement the necessary processes to train its staff in cybersecurity.

The model includes the following components:

- **Maturity levels**. They represent different levels of organizational capability for managing and developing the training, skills, and competences processes to generate a cybersecurity culture inside an energy company.
- **Processes**. Each maturity level, with the exception of the Initial Level, consists of four processes, which identify the capabilities that must be defined and deployed in the company to achieve a maturity level.

- **Practices**. Processes include a set of practices that are needed for achieving the process goal.
- **Tips**. Advices or evidence examples that can help the company to define and deploy a specific practice. They can be seen also as evidence example to verify that the practice is being carried out.

Figure 15 shows the different components of the Maturity Model and the relationship among them.

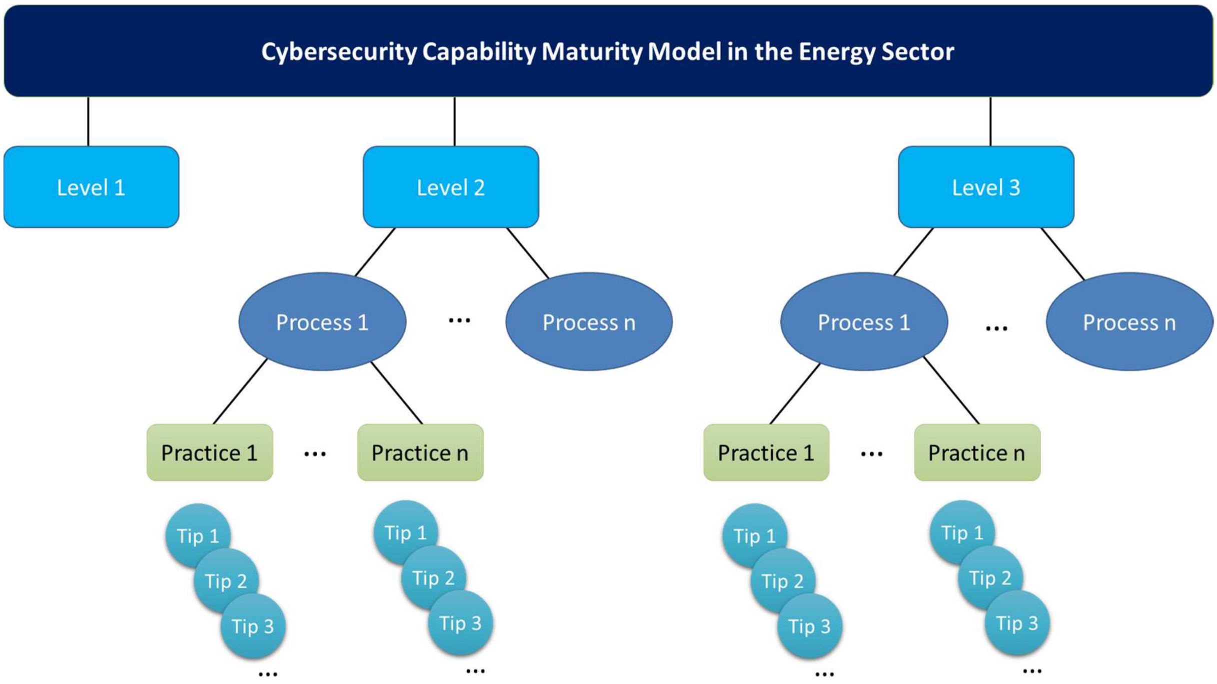


Figure 15. Components of the SDN-microSENSE Cybersecurity Capability Maturity Model

4.3 Maturity Levels

The first component of the model is the maturity levels. They represent different levels of organizational capability for managing and developing the training, skills and competences processes to generate a cybersecurity culture inside an energy company.

SDN-microSENSE Cybersecurity Capability Maturity Model considers 3 maturity levels:

- Initial level, where processes, although can exist in the organisation, are not defined or not homogenously defined and deployed. All companies are in this initial level by default.
- People Managed level, where processes oriented to the personnel cybersecurity training management are defined and deployed.
- Competency managed, where processes oriented to the cybersecurity competences management are defined and deployed.

Figure 16 shows the maturity levels of the SDN-microSENSE CCMM.

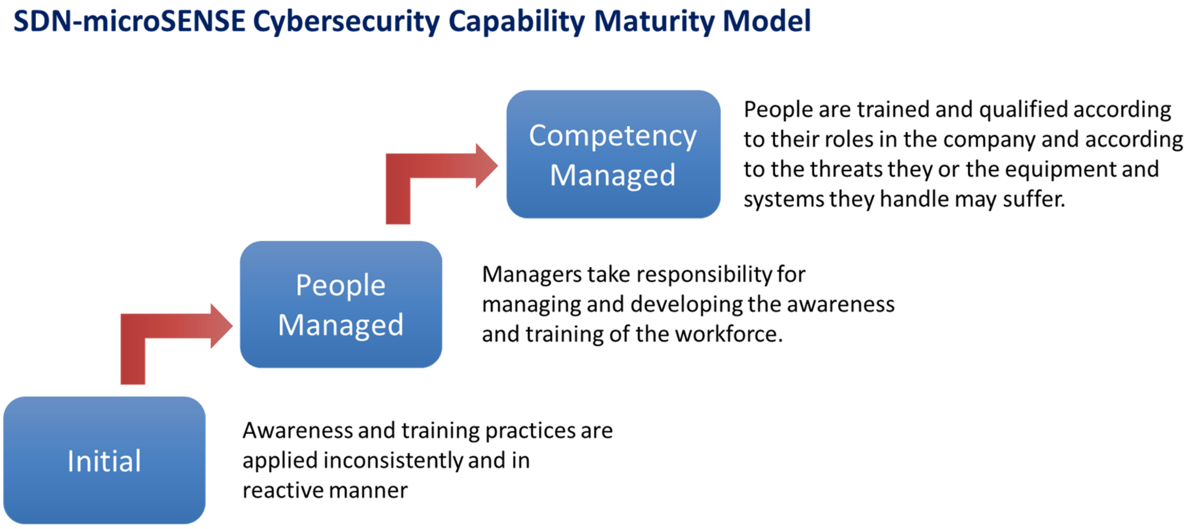

SDN-microSENSE Cybersecurity Capability Maturity Model
Competency Managed
People are trained and qualified according to their roles in the company and according to the threats they or the equipment and systems they handle may suffer.
People Managed
Managers take responsibility for managing and developing the awareness and training of the workforce.
Initial
Awareness and training practices are applied inconsistently and in reactive manner

Figure 16. Maturity levels of the SDN-microSENSE Cybersecurity capability maturity Model

Table 13 analyse the way the following aspects are considered in each maturity level:

- The formalisation of the training and awareness processes.
- Communication and coordination practices.
- The work environment.
- The incorporation of cybersecurity competences as part of personnel competency.

Table 13. Maturity Levels

Topics / Disciplines	Initial	People Managed	Competency Managed
Training and awareness processes	Not formalized at organisational level Personnel are not sufficiently aware of the precautions they should take.	Formalised but not individualised. Cybersecurity awareness is promoted based on general information and best practices.	Individualised to each user role. Organization adapts its training practices based on lessons learned and risk assessment.
Communication and Coordination	There are not processes to transmit and share information about detected cybersecurity risk and incidents	Mechanisms to report and share risks and incidents are established.	Participatory culture

Topics / Disciplines	Initial	People Managed	Competency Managed
Work Environment	Does not have cybersecurity working conditions	Companies deploy basic cybersecurity working conditions to allow individuals to perform their cybersecurity tasks efficiently, and to avoid unintentional incidents. At this level Companies also deploy cybersecurity basic measurements.	Companies deploy consistent working conditions to allow individuals to perform their cybersecurity tasks efficiently based on planned process Specific measurements are adopted based on a risk assessment process.
Cybersecurity Competences	Has not been identify.	Are part of the personnel competences in each role and are considered in the staffing processes (recruiting, compensating)	Based on a competency analysis of each user role.

Figure 17 shows the processes defined in each maturity level.

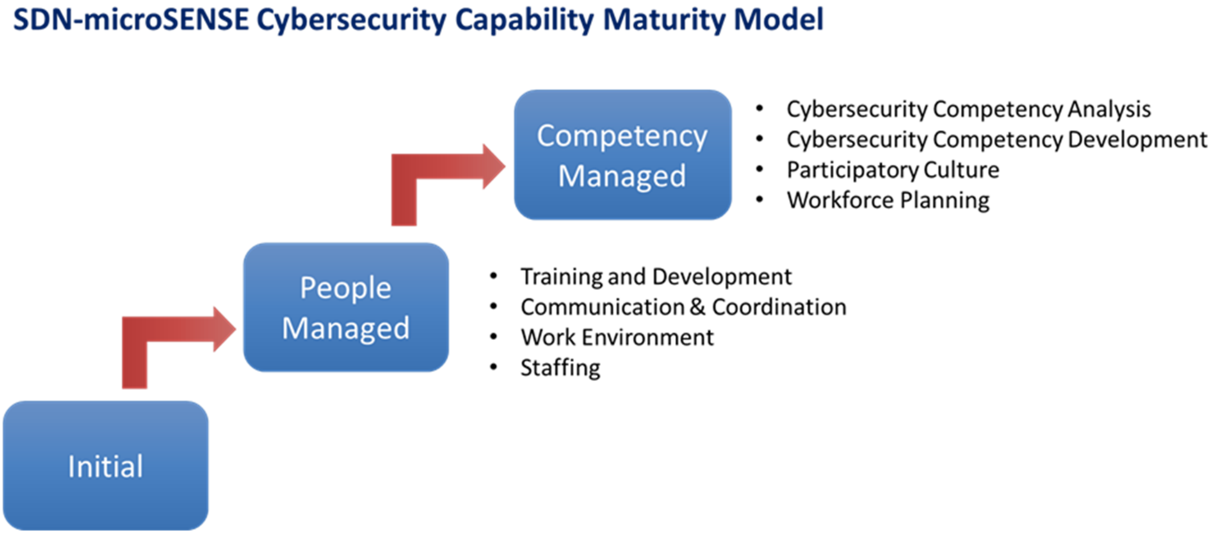

SDN-microSENSE Cybersecurity Capability Maturity Model
Competency Managed
Cybersecurity Competency Analysis
Cybersecurity Competency Development
Participatory Culture
Workforce Planning
People Managed
Training and Development
Communication & Coordination
Work Environment
Staffing
Initial

Figure 17. Process defined in each maturity level.

4.3.1 Initial Level

Organizations at the Initial Level present the following situation:

- Cybersecurity training practices are not formalized at organisational level, and awareness is managed in an ad hoc and sometimes reactive manner, for example after a cyberattack in the company or in the society.
- There is limited concern about cybersecurity risk and personnel are not sufficiently aware of the precautions they should take, for example, when opening emails, connecting external devices to the laptop, executing field maintenance operation, etc.
- There are not processes to transmit and share information about detected cybersecurity risk and incidents, and this information are not shared with other entities.
- Organisation has not identified cybersecurity capabilities (knowledge, skills and abilities) in each workplace.
- In general, processes could be executed but without formalism and sometimes chaotically.
- Good results in terms of cybersecurity management depend on additional efforts made by the most capable people.
- Exceptional results in terms of cybersecurity activities execution can be achieved, as long as the best people are assigned to these tasks.

At this level there are not defined and managed process.

4.3.2 People Managed Level

Organizations at the People Managed Level present the following situation:

- There is an awareness of cybersecurity risks and activities at the organizational level.
- Training and awareness policies, processes and procedures related to cybersecurity practices are defined and implemented
- Staff has adequate resources to perform their cybersecurity duties.
- Cybersecurity information is shared within the organization on a formal basis.
- The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally.
- Responsibilities and authorities related to cybersecurity activities execution are assigned depending on needs in terms of cybersecurity.
- Previous successes related to cybersecurity risk management and practices are repeatable in the future
- Discipline helps to maintain cybersecurity practices in times of stress
- Managers have visibility of cybersecurity activities and results.

Frequent problems that keep people from performing effectively in low-maturity organizations include work overload, environmental distractions, unclear performance objectives or feedback, lack of relevant knowledge or skill, poor communication, and roles and responsibilities not defined.

Special attention is put on managers. The first step toward improving cybersecurity competencies of the personnel is to get managers to take workforce activities regarding cybersecurity issues as high-priority responsibilities of their job. It is difficult to implement organization wide practices if managers are not performing the basic workforce practices required to manage their units.

The practices implemented at People Managed Level focus a manager's attention on unit-level issues such as staffing, coordinating commitments, providing resources, managing performance, developing skills, and making compensation decisions related to cybersecurity issues.

4.3.3 Competency Managed Level

Organizations at the Competency Managed Level presents the following situation:

- Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner
- There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.
- Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks
- The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs
- The primary objective of the Competency Managed Level is to help an organization gain a competitive advantage by developing the various competencies that must be combined in its workforce to accomplish its business activities.
- Each workforce competency represents a distinct integration of the knowledge, skills, and process abilities required to perform some of the business activities that contribute to an organization's core competency.
- The members of the organization's workforce who share the knowledge, skills, and process abilities of a particular workforce competency constitute a competency community.

4.4 People Managed Processes

A process identifies the capabilities that must be defined and deployed in the company to achieve a maturity level. In the People Managed Level, the organization establishes a cybersecurity culture focused at the user role level for ensuring that people know the main cybersecurity functions associated to their role in the company and that adopt the required cybersecurity measurements.

In achieving People Managed Level, the organization develops the capability to manage cybersecurity skills and performance at the user role level.

The processes in the People Managed Level are:

1. Training and development.
2. Staffing.

3. Work environment.
4. Communication and coordination.

4.4.1 Training and Development

Table 14 provides the description of the Training and Development process of level 2. The information containing in the table has been elaborated starting from the Training and Development Process Area defined in People CMM[13]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 14. Process description: Training and Development

Process	Training and Development
The purpose of Training and Development is to ensure that all individuals have the knowledge and skills required to perform their assignments and activities related to cybersecurity. The primary focus of Training and Development is on removing the gap between the current skills of each individual and the skills required to perform their assignments related to cybersecurity activities. Roles involved in the process deployment: Members of the human resources function or Unit Managers or a group leader.	
Objectives	
Objective 1	Individuals receive timely training that is needed to perform their work.
Practices	
Practice 1	Identify cybersecurity knowledge and skills required for performing each individual's assigned tasks. TIP: • Maintain records of knowledge and skills required.
Practice 2	Identify the training needed in critical cybersecurity skills for each individual. TIP: • The term "Critical Cybersecurity Skills" refers to: 1. Execute specific cybersecurity procedures 2. Use equipment effectively
Practice 3	Each unit develops and maintains a plan for satisfying its training needs. TIP: • The unit's training plan typically specifies: 1. Training needed by each individual or workgroup to perform their assigned responsibilities. 2. Training to be provided to individuals or workgroups to support their development interests. 3. The schedule for when training is to be provided. 4. How this training is to be provided

[13] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

Practice 4	Individuals or groups receive timely training needed to perform their assigned tasks. TIP: • Examples of training alternatives include the following: 1. Classroom training 2. Distance learning 3. Mentoring 4. Apprenticeships 5. Self-paced learning courses
Practice 5	Training is tracked against the unit's training plan.
Practice 6	A development discussion is held periodically with each individual. TIP: • Information about knowledge and skills can come from the following: 1. Evidence from current performance 2. Changing requirements of the current assignment 3. Anticipated future assignments 4. Individual desire to know more in an area relevant to the organization 5. Recommendations from others 6. Individual desire for reassignment or advancement
Practice 7	Relevant development opportunities are made available to support individuals in accomplishing their individual development objectives. TIP: • Examples of development opportunities include the following: 1. Courses 2. Degree or certification programs 3. Mentors or coaches 4. Special temporary assignments 5. Position or role assignments
Practice 8	Individuals pursue development activities that support their individual development objectives.
Practice 9	Managers review the training activities status and results.
Practice 10	Measurements are made and used to determine the status and performance of Training and Development activities TIP: Examples of measurements include the following: • Amount of training provided • Rate of training against stated training needs • Timeliness of training • Cost of training, Quality of training as rated in student evaluations.

4.4.2 Staffing

Table 15 provides the description of the Staffing Process of level 2. The information containing in the table has been elaborated starting from the Staffing Process Area defined in People CMM[14]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 15. Process description: Staffing

Process Area	Staffing
The purpose of Staffing is to establish a formal process by which committed work regarding cybersecurity needs is matched to unit resources and qualified individuals are recruited, selected, and transitioned into assignments. Roles involved in the process deployment: Members of the human resources function or Resource managers and Unit manager	
Objectives	
Objective 1	Individuals or workgroups in each unit are involved in making commitments that balance the unit's workload with approved staffing.
Objective 2	Candidates are recruited for open positions.
Objective 3	Staffing decisions and work assignments are based on an assessment of work qualifications and other valid criteria.
Objective 4	Individuals are transitioned into and out of positions in an orderly way.
Practices	
Practice 1	Each unit analyses its work to determine the cybersecurity skills required. TIPs: • A unit's work is analysed to determine the types of tasks that requires cybersecurity measurements and effort required to perform them. • The types of skills (cybersecurity skills) needed to perform proposed work are identified.
Practice 2	Individuals and workgroups participate in making commitments for cybersecurity measurements *they have to adopt and perform*. TIPS: • Individuals are involved in reviewing the cybersecurity measurements to be adopted in their work • Individuals or workgroups are involved in estimating the resources, effort, and schedule required to deploy cybersecurity measurements to accomplish the work that they have been allocated. • Individuals or workgroups establish commitments they will be held accountable for meeting. • Individuals or workgroups are involved in reviewing progress against commitments and, when necessary, making changes to the commitments regarding their work.
Practice 3	Each unit documents cybersecurity commitments that balance its workload with available staff and other required resources.

[14] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

Practice 4	Individual cybersecurity assignments are managed to balance committed cybersecurity measurements among individuals and units or groups.
Practice 5	Position openings regarding cybersecurity needs within a unit are analysed, documented, and approved.
Practice 6	Position openings regarding cybersecurity needs within the organization are widely communicated.
Practice 7	Units with open positions regarding cybersecurity needs recruit for qualified individuals.
Practice 8	External recruiting activities regarding cybersecurity needs by the organization are planned and coordinated with unit requirements.
Practice 9	A selection process and appropriate selection criteria are defined for each open position regarding cybersecurity needs. TIP: • Selection criteria are defined from: the tasks, job characteristics, and work conditions of the open position; characteristics of candidates who are capable of performing the work responsibilities of the open position, other skill needs of the unit or organization, and other staffing objectives of the organization • Examples of activities for evaluating candidates include the following: Individual interviews; Group interviews; Formal structured interviews; Presentations; Sample tasks
Practice 10	Each unit, in conjunction with its human resources function, conducts a selection process for each position regarding cybersecurity needs it intends to fill.
Practice 11	Positions regarding cybersecurity needs are offered to the candidate whose skills and other qualifications best fit the open position.
Practice 12	The organization acts in a timely manner to attract the selected candidate. TIP: Examples of the terms of the offer that can be negotiated include the following: Job level and title, Salary and benefits, Probationary period, Relocation, Training
Practice 13	The selected candidate is transitioned into the new position. TIP: Examples of transition activities include the following: Preparing an office and required equipment, selecting an orientation mentor, Meeting existing members of the unit, Orientation to the job, Orientation to the organization, etc.
Practice 14	Representative members of a unit participate in its staffing activities. TIP: • Examples of staffing activities in which members of the unit can participate include the following: Identifying characteristics of qualified candidates, Recruiting, referring potential candidates, screening potential candidates, Evaluating qualified candidates.
Practice 15	Workforce reduction and other outplacement activities regarding cybersecurity needs, when required, are conducted according to the organization's policies and procedures. TIP:

	Examples of reasons for outplacement include the following: Loss of budget or work, Shifts in skill needs, Changes in location of facilities
Practice 16	Discharges for unsatisfactory performance regarding cybersecurity issues or other valid reasons are conducted according to the organization's policies and procedures. TIP: Examples of reasons for discharge could include the following: Unsatisfactory performance, Misconduct
Practice 17	Causes of voluntary resignation from the organization are identified and addressed.
Practice 18	Managers review the staffing activities status and results.
Practice 19	Measurements are made and used to determine the status and performance of Staffing activities: TIP: Examples of measurements include the following: • Number of open positions identified • Number of qualified candidates contacted through each recruiting source • Percent of qualified candidates contacted directly by staff rather than through other sources • Percentage of selected candidates accepting offers • Cost per hire

4.4.3 Work Environment

Table 16 provides the description of the Working Environment Process of level 2. The information containing in the table has been elaborated starting from the Work Environment Process Area defined in People CMM[15]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 16. Process description: Work Environment

Process	**Work Environment**
The purpose of Work Environment is to establish and maintain physical working conditions and to provide resources that allow individuals and workgroups to perform the detection of intrusions efficiently and also to avoid unintentionally security incidents caused by the personnel. This process focuses on both the resources provided for performing work (e.g., firewalls, access control systems, secured communication protocols, intrusion detection tools, information protection), and the physical conditions in which the work is performed (e.g., physical access control to installations). The work environment must be managed to ensure it supports the tasks required to assure the security measurements that avoid any kind of security incidents. This process focuses on both the	

[15] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

resources provided for supporting the personnel in the security tasks, and the physical conditions under which these tasks are performed. Management must balance expenditures on resources and environment with justifications based on the work being performed. Management should have also plans for mitigating the potential problems judged to present serious risks to health, safety, or efficiency. Roles involved in the process deployment: Physical plant or facilities staff, Telecommunications staff, Computing facilities staff, etc.	
Objectives	
Objective 1	To provide the physical environment and resources needed by the personnel to detect cyber incidents and avoid unintentionally security incidents
Objective 2	To create an appropriate environment to minimise the distractions in the work, this will allow to have less security incidents and unintentionally security incidents
Practices	
Practice 1	The physical environment and resources required to detect potential cyber-security incidents are identified for each role. TIP: • Depending on the role of the employee this physical environment should be changed. The resources to be considered are different if the role works in a control room or a substation or an office. • These resources could include the following: Individual, group and meeting space, telecommuting support, support for remote locations, special characteristics of physical workspaces, communication equipment, computer and software tools. • Preparing budget requests for the needed physical environment or other resources • Coordinating actions needed to implement the improvements consulting with appropriate subject matter experts
Practice 2	The physical environment required to detect the cyber security incidents is provided according to the identification done in practice 1. An adequate space should be provided, this means to design the space for supporting the efficient performance of the detection of cyber incident and the security tasks derived. If the most adequate physical space is not able to be provided, some mitigation actions should be implemented. TIP: • Some characteristics to consider in order to provide secure physical space: Control access, video protection, visibility, noise, voice communication and so on.
Practice 3	An adequate personal environment for detecting cybersecurity incidents and for avoiding unintentionally security incidents is provided. TIP: • This personal environment should assure: ▪ Protected private space where personal effects, work tools, and products can be secured and stored as necessary

	▪ Adequate desktop space for using tools and other resources in performing tasks. ▪ Enough isolation and noise protection to support the level of concentration needed to perform individual work. ▪ Enough space to perform work activities alone or with a limited number of colleagues, as appropriate.
Practice 4	The specialized resources that would normally be available for performing the detection of cybersecurity incidents are made available and adequate support is provided. TIPS: • In order to detect cybersecurity incidents in the organisation a specialised resource could be an intrusion detection system that informs that a potential intrusion could be occurred • Other resource that could help is to set up security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of the systems
Practice 5	Improvements are made to the work environment that improve the detection of cybersecurity events. TIP: • The efficiency of this work environment when detecting security events is analysed to identify potential changes or resources that could improve the performance. • It is important to prioritise the improvements. This prisonisation should consider different aspects: impact, budget, laws and regulations and so on
Practice 6	Physical factors that degrade the effectiveness of the work environment are identified and addressed. TIP: • Analyse all the factors that can affect to the environment set up to detect cybersecurity incidents. These factors could be from different nature from the excessive noise to the malfunction of the control access mechanism both digital and physical ones.
Practice 7	Sources of frequent interruption or distraction that can generate unintentionally security incidents are identified and minimized. TIP: • Some factors that can generate distractions are: Telephone calls, excessive meetings, poorly organized work processes, unnecessary or excessive administrative tasks, work that could be performed by other, more appropriate, individuals…
Practice 8	Managers review the work environment activities status and results.
Practice 9	Measurements are made and used to determine the status and performance of Work Environment activities TIP: Examples of measurements include the following: • Number of complaints or concerns raised about the work environment • Number of violations of work environment laws or regulations • Effectiveness of improvements on performance

	• Investment in work environment improvements

4.4.4 Communication and Coordination

Table 17 provides the description of the Communication and Coordination Process of level 2. The information containing in the table has been elaborated starting from the Communication and Coordination Process Area defined in People CMM[16]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 17. Process description: Communication and Coordination

Process Area	Communication and Coordination
The purpose of Communication and Coordination is to establish timely communication throughout the organization and to ensure that the personnel has the skills to share cybersecurity information *(risks, security breaches and cyber incidents)* and that this information are efficiently coordinated. Roles involved in the process deployment: Physical plant or facilities staff, Telecommunications staff, Computing facilities staff, etc.	
Objectives	
Objective 1	Cybersecurity Information is shared across the organization.
Objective 2	Individuals or groups are able to raise cybersecurity concerns and have them addressed by management.
Objective 3	Individuals and workgroups coordinate their activities to detect cybersecurity risks, reduce vulnerabilities and respond to incidents.
Practices	
Practice 1	The workforce-related policies and practices of the organization are communicated to the workforce. TIPS: Individuals and units are informed of policies and practices that affect them: • Security policy of the company • Individual and unit responsibilities, • Procedures for notifying any security risk, bad practice or breach. Whenever people-related policies and practices are changed, the changes are communicated to the workforce. Possible ways to perform this communication: 1.- General Meetings. 2.- Periodical reminders in the unit meetings. 3.- Use of posters
Practice 2	Information about cybersecurity values, events, and conditions is communicated to the workforce on a periodic and event-driven basis. TIPS: Examples of information that is to be communicated: 1. Organizational mission, vision, and strategic objectives 2. Business ethics

[16] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

	3. Security plans and objectives 4. Security performance 5. Changes in cybersecurity organizational structure or processes (Security Admin for example) 6. Notable cybersecurity events, risk, activities, infrastructure, etc. Communication mechanisms: 1.- Organization-wide meetings 2.- Staff meetings 3.- One-on-one meetings 4.- Bulletin boards 5.- Electronic mail announcements 6.- Internal publications 7.- Newsletters 8.- Memos
Practice 3	Information required for performing committed work in a secure way is shared across affected units in a timely manner. TIPS: Information about: 1. New detected threats and vulnerabilities. 2. The results of risk assessments processes. 3. New tools and process deployed in the company to increase cybersecurity.
Practice 4	Individuals' opinions on their security working conditions are sought on a periodic and event-driven basis. Inputs are analysed and the results, decisions, and actions are communicated. To ensure confidentiality, results are presented so that individuals or groups cannot be identified as the source of information unless they have given their permission to be identified TIP: The company has established the following procedures: 1. Immediate notification of any aspect that may suppose a cybersecurity risk. 2. Group meetings 3. Cybersecurity incident review. 4. Email or other electronic means 5. Suggestion boxes or other private means
Practice 5	Individuals or groups can raise concerns related to cybersecurity issues according to a documented procedure. TIP: The company has set up mechanisms or procedures to allow people to raise concerns related with cybersecurity. 1.- A tool for collecting concerns and complaints.
Practice 6	Activities related to the resolution of a cybersecurity problems are tracked to closure. TIP: 1. Responsibilities are assigned for tracking the status of concerns.

	2. The status of all open concerns is periodically reviewed by management. 3. When appropriate progress has not been made in resolving a concern, corrective action is taken.
Practice 7	Individuals and workgroups monitor and coordinate the dependencies involved in their committed work. TIP: Where the work is interdependent, individuals and workgroups should ensure they mutually agree to their commitments in order to coordinate their activities. 1. Identify dependencies. 2. Create dependencies. 3. Coordinate dependent work. 4. Document dependencies.
Practice 8	Meetings are conducted to make the most effective use of participants' time.
Practice 9	Managers review the Communication and Coordination activities status and results.
Practice 10	Measurements are made and used to determine the status and performance of Communication and Coordination activities TIP: Examples of measurements include the following • Results from opinion surveys • Number of conflicts handled through formal mechanisms • Number of concerns raised

4.5 Competency Managed Processes

In the Competency Managed level the organization identifies and develops the knowledge, skills, and process abilities that constitute the workforce competencies required to perform its business activities with the maximum level of cybersecurity. The organization develops a cybersecurity culture of professionalism based on well-understood workforce competencies. In this level the organization develops the capability to manage its workforce as a strategic asset.

The processes in the Competency Managed level are:

1. Cybersecurity Competency Analysis
2. Cybersecurity Competency Development
3. Workforce Planning
4. Participatory Culture.

4.5.1 Cybersecurity Competency Analysis

Table 18 provides the description of the Cybersecurity Competency Analysis Process of level 3. The information containing in the table has been elaborated starting from the Competency Analysis

Process Area defined in People CMM[17]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 18. Process description: Cybersecurity Competency Analysis.

Process Area	***Cybersecurity* Competency Analysis**
The purpose of Competency Analysis is to: 1. Identify the cybersecurity knowledge, skills, and process abilities required to perform the organization's business activities in the in the most security possible way. 2. Maintain descriptions (*the organisation should maintain*) of the cybersecurity knowledge, skills, and process abilities that comprise each workforce competency. 3. Set up an organizational repository where these descriptions are maintained and available. 4. Assess these descriptions periodically to ensure they remain current with the organization's technologies and business activities. 5. Define, and update as necessary, the work processes used by capable individuals in each workforce competency. Roles involved in the process deployment: Member of Human resources, Managers o Engineering groups focused in cybersecurity, etc.	
Objectives	
Objective 1	The cybersecurity competencies required to perform a business activity are defined and updated.
Objective 2	The cybersecurity measures used within each workforce competency are defined and maintained.
Objective 3	The organization tracks *cybersecurity* capability in each of its user roles competencies.
Practices	
Practice 1	The cybersecurity competencies required to perform the organization's business activities are identified and analysed to identify the knowledge, skills, and process abilities that compose them TIP: For each role 1. Cybersecurity knowledge, skills, and process abilities required to perform committed work are defined for each business activity. 2. SDN-microSENSE Cybersecurity Competency Model can be used. 3. Subject matter experts are involved in analysing the cybersecurity knowledge, skills, and process abilities required to perform their committed work. 4. A description of the cybersecurity knowledge, skills, and process abilities is defined for each business activity
Practice 2	Workforce competency descriptions are documented and maintained according to a documented procedure.

[17] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

	TIP: 1.- Cybersecurity competency descriptions are controlled and maintained under version control.
Practice 3	Cybersecurity competency descriptions are updated on a periodic and event driven basis. TIP: 1. Cybersecurity competencies are periodically reanalysed to determine if they continue to reflect the knowledge, skills, and process abilities necessary to perform the organization's business activities. 2. Changes in products, services, processes, or technology are analysed as necessary to determine whether affected cybersecurity competency descriptions need to be updated, new competencies need to be defined, or obsolete cybersecurity competencies need to be phased out.
Practice 4	The competency-based cybersecurity processes to be performed by capable individuals in each workforce competency are established and maintained. TIP: 1.- Competency-based cybersecurity processes are documented and made available for guiding those developing or performing a workforce competency. 2.- Documented competency-based *cybersecurity* processes are updated on an event-driven basis to reflect • changes in business operations, products, or services, • changes in other processes or development technologies, • lessons learned from the performance of competency-based processes, • other process improvements.
Practice 5	Current resource profiles for each of the organization's workforce competencies are determined. A resource profile for a workforce competency represents the number of individuals at each level of capability within the workforce competency. An example of progressive levels of capability within a workforce competency may include a beginner, a novice, a journeyman, a senior practitioner, and a master or expert. TIP: 1. Competency information is aggregated at the organizational level for each of the organization's cybersecurity competencies. 2. The organization uses aggregated competency information to develop a resource profile for each of the organization's cybersecurity competencies. 3. Resource profiles are made available, as appropriate, for use in workforce planning, the analysis of workforce practices, and other workforce activities.
Practice 6	Competency information is updated on a periodic and event-driven basis. TIP: 1. Competency information for an individual (or other unit of analysis) may be updated as accomplishments, experience, or events justify.

	2. Competency information for affected individuals should be updated as appropriate when workforce competency descriptions are modified, added, or phased out.
Practice 7	Managers review the Cybersecurity Competency Analysis activities status and results.
Practice 8	Measurements are made and used to determine the status and performance of Communication and Coordination activities: TIP: Number of workforce competencies identified and analysed, number of actions identified to obtain the appropriate workforce competencies, effort spent in the cybersecurity competency activities, etc.

A specific Competency Analysis is done in Section 5 as a Guidelines for EPES companies.

4.5.2 Cybersecurity Competency Development

Table 19 provides the description of the Cybersecurity Competency Development Process of level 3. The information containing in the table has been elaborated starting from the Competency Development Process Area defined in People CMM[18]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project

Table 19. Process description: Cybersecurity Competency Development.

Process Area	Cybersecurity Competency Development
The purpose of Cybersecurity Competency Development is to enhance constantly the capability of the workforce to perform its assigned tasks and responsibilities. The cybersecurity competencies identified in Competency Analysis and the needs identified in Workforce Planning provide the foundations for the organization’s competency development program. Graduated training and development opportunities are designed to support development in each of the organization’s workforce competencies. Individuals pursue competency development opportunities that support their individual development objectives. The organization uses the experience of its workforce to develop additional capability in each of its workforce competencies through practices such as mentoring. Mechanisms are established to support communication among the members of a competency community. Roles involved in the process deployment: Member of Human resources, Managers or Engineering groups focused in cybersecurity, etc.	

[18] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

Objectives	
Objective 1	The organization provides opportunities for individuals to develop their cybersecurity capabilities in its workforce competencies. Individuals develop their knowledge, skills, and process abilities in the organization's workforce competencies.
Objective 2	The organization uses the cybersecurity capabilities of its workforce as resources for developing the workforce competencies of others.
Practices	
Practice 1	Cybersecurity competency development activities are based on the competency development plans within each workforce competency. TIP: • Cybersecurity Competency development activities are selected and based on a competency development plan. • Cybersecurity Competency development activities are prioritized to align with the organization's measurable objectives and the competency development plan.
Practice 2	Graduated training and development activities are established and maintained for developing *cybersecurity* capability in each of the organization's workforce competencies. TIP: 1. Graduated training and development activities are identified. Examples of competency development activities include the following: • Formal classroom training • Courses of study at educational institutions • Degree programs • Licensing or certification programs • Guided self-study • Apprenticeship or mentoring • Just-in-time training • Workgroup (or team) training and development activities • Knowledge repositories and tools • Career development planning 2. The organization establishes standards for the learning activities. 3. Learning activities are periodically reviewed. 4. Resources for delivering the training and development activities are identified and made available. 5. The training and development program is updated as changes are made to profiles of the organization's workforce competencies. 6. Training and development records are maintained at the organizational level
Practice 3	Cybersecurity Competency-based training and development activities are identified for each individual to support their development objectives. TIP: 1. A responsible individual(s) helps each individual identify cybersecurity competency-based training and development needs and ensures that

	appropriate competency development activities are identified, planned, and performed. 2. A responsible person counsels individual, as needed, about available training and development
Practice 4	Individuals actively pursue learning opportunities to enhance their capabilities in cybersecurity competencies. TIP: 1. Individuals are encouraged to take the initiative in pursuing *cybersecurity* competency development opportunities. 2. Individuals ensure their *cybersecurity* competency information is updated when *cybersecurity* competency development activities are completed
Practice 5	Capable individuals within a competency community are used to mentor those with less capability in the *cybersecurity* competency. TIP: 1. Elaborate a list of people in the organisation that can be used as mentors. 2. Individuals willing to act as mentors are prepared to perform their responsibilities. 3. Mentors and those being mentored establish arrangements for conducting their mentoring relationship. 4. Mentors provide timely feedback and guidance to those they mentor.
Practice 6	The organization supports communication among those comprising a cybersecurity competency community. The members of a workforce that share the common cybersecurity knowledge, skills, and process abilities of a particular business activity or role constitute a cybersecurity competency community. TIP: Examples of mechanisms for supporting communication within a cybersecurity competency community include the following: • Periodic meetings • Informal discussions • Professional activities • Social gatherings • Peer group reviews, boards, and similar activities • Periodic newsletters or bulletins • Updated technical, process, or business documentation • Electronic bulletin boards, web pages, and other forms of computer-mediated communication and networking • Information repositories
Practice 7	Managers review the Cybersecurity Competency Development activities status and results.
Practice 8	Measurements are made and used to determine the status and performance of Cybersecurity Competency Development activities: TIP:

	Amount of time spent in developing the knowledge, skills, and process abilities underlying the organization's cybersecurity workforce competencies, Number of people and amount of effort involved in developing or delivering Cybersecurity Competency Development activities, Amount and types of communication within a competency community, etc.

4.5.3 Workforce Planning

Table 20 provides the description of the Workforce Planning Process of level 3. The information containing in the table has been elaborated starting from the Workforce Planning Process Area defined in People CMM[19]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 20. Process description: Workforce Planning

Process	**Workforce Planning**
The purpose of Workforce Planning is to coordinate workforce activities with current and future cybersecurity needs at both the organizational and role levels. Through workforce planning, the organization identifies the workforce it needs for its current and future activities oriented to detect and stop the cybersecurity incidents and plans the actions to be taken to ensure the required workforce is available when needed. Roles involved in the process deployment: Member of Human resources or Managers.	
Objectives	
Objective 1	Establish measurable objectives for capability in each of the organization's cybersecurity workforce competencies are defined.
Objective 2	The organization plans for the workforce competencies needed to perform its current and future oriented to detect and stop the cybersecurity incidents
Objective 3	Each role performs workforce activities to satisfy current and strategic competency needs.
Practices	
Practice 1	The current and strategic cybersecurity workforce needs of the organization are documented. TIP: • Inputs required to identify these needs are collected and documented. Some examples: ○ the number of people required to accomplish the role´s committed work compared to the number available, ○ the workforce competencies needed to conduct the cybersecurity activities constituting these commitments compared to the unit's current capability in these workforce competencies,

[19] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

	○ the unit's anticipated future commitments that have current staffing implications.
Practice 2	Measurable objectives are established for developing the organization's capability in each of its selected workforce competencies. TIP: • Examples of measurable objectives: ○ Level of knowledge, skill, and process ability available in each of the security workforce competencies ○ The rate at which knowledge, skill, and process ability are acquired in each of the security workforce competencies ○ The deployment of the security workforce competencies across the organization ○ The rate at which new security workforce competencies can be developed and deployed across the organization
Practice 3	A competency development plan for cybersecurity concepts and information on how to detect these attacks is produced and reviewed by all the involved people on a periodic and event-driven basis. A guideline about the competencies by role in an EPES is described in the annex 1. TIP: • Information to be added in this plan: ○ measurable objectives for developing capability in the workforce competency, ○ the number of people anticipated or required with the needed competency over the period covered by the plan, ○ how the number of people with the competency will be developed or staffed. • It is important that the plan for the competency in cyber security is incorporated into the organization's strategic workforce plan and provide input to planned workforce activities by units.
Practice 4	The organization establishes and maintains a strategic workforce plan to guide its workforce practices and activities related to detect potential cybersecurity. TIP: • These activities may include developing specialists within the competency, providing minimal training to all individuals to achieve a base-level competency (Example of this can be found on the annex 1) , retraining individuals or groups whose competencies may become obsolete or oversupplied, providing cross-training for selected individuals, or training selected groups within units • Staffing activities to reallocate or recruit individuals necessary to meet the current and strategic workforce needs of the organization (see Staffing process). • Some compensation activities could be defined to motivate development or retention of needed competencies
Practice 5	Roles plan workforce activities to satisfy competency needs to be able to detect cybersecurity attacks in an efficient way. The plans are reviewed on a periodic and

	event-driven basis. TIP • For each role in the organisation performance objectives should be defined and documented: ○ developing the competencies needed to perform its security activities, ○ contributing to the security competency development objectives of the organization, and ○ performing planned activities that support these competence development objectives. • It is important that all the roles revise their plans for workforce activities according to documented procedures.
Practice 6	Progress in meeting the objectives of the competency development plan for each of the cybersecurity competencies is tracked. TIP: • Individual or group is assigned responsibility for tracking performance against its competency development plan. If results deviate significantly from the competency development plan for a competency, corrective action is taken.
Practice 7	Each role´s performance in conducting its planned workforce activities is tracked. TIP • Each role periodically reviews its status in performing planned workforce activities. • The progress of each role in executing its planned workforce activities is periodically reviewed at the organizational level. • Corrective actions are taken when results deviate significantly from a role’s objectives in performing its planned workforce activities.
Practice 8	Managers review the Workforce Planning activities status and results.
Practice 9	Measurements are made and used to determine the status and performance of Workforce Planning activities: TIP: Examples of measurements include the following: • Time spent in organizational and role level workforce planning • Number of people involved in Workforce Planning activities • Effectiveness of meeting milestones in workforce planning • Effectiveness of achieving the objectives of the strategic workforce plan • Effectiveness in performing workforce activities at the organizational and role levels

4.5.4 Participatory Culture

Table 21 provides the description of the Participatory Culture Process of level 3. The information containing in the table has been elaborated starting from the Participatory Culture Process Area defined in People CMM[20]. The information has been adapted to the Cybersecurity Context of the SDN-microSENSE project.

Table 21. Process description: Participatory Culture

Process	**Participatory Culture**
The purpose of a participatory Culture is to enable the workforce's full capability for making decisions that affect the performance of business activities oriented to detect cybersecurity risks. A participatory culture about aspects related with security provides an environment in which competent professionals are fully able to exercise their capabilities focused on cybersecurity aspects. This participative environment ensures a flow of information when a security alarm is detected within the organization, incorporates the knowledge of individuals into decision-making processes, and gains their support for commitments. Establishing a participatory culture begins with providing individuals and workgroups with information about cyber security activities performance. Individuals and workgroups are provided access to the information needed to perform their committed work. Roles involved in the process deployment: Member of Human resources or Executive management.	
Objectives	
Objective 1	Information about cybersecurity activities and results is communicated throughout the organization.
Objective 2	Decisions about the security aspects are delegated to an appropriate level of the organization and individual or workgroups participate in the decision-making processes
Practices	
Practice 1	Information about cybersecurity tasks performance is made available to individuals and workgroups TIP: • Identify the relevant information related to the cybersecurity activities performance: objectives, performance data of the preventing activities, information regarding changes in the work environment, cost of the activities, budget for new security measures • It should be detailed the level of information provided to each role and the frequency of this information • It important to consider the information that should be treated as confidential
Practice 2	Individuals and workgroups are made aware of how their work in the security aspects contributes to cybersecurity tasks performance TIP: • The information regarding the performance of the task as informed at all the levels: individual and workgroups • The information regarding the link between individual, workgroup, unit, and organizational performance in the detection of intrusion and other activities related with cybersecurity are explained.

[20] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5329

Practice 3	Individuals and workgroups have access to information needed to perform their tasks regarding on the security aspects and to the systems that support the access to this information. TIP: • The information that should be provided is: Assigned tasks and responsibilities, standard processes, workgroup coordination, assigned or assumed roles and dependencies. Also, the mechanism on how this information is transferred and ensure the correct coordination with information sources to ensure timely access • The communication system should broaden and accelerate the flow of information needed to enhance the activities to detect the cybersecurity incident and the speed and accuracy of decisions • It is important to facilitate the participation of the all the people involved in decisions about improvements and upgrades to the information and communication technologies that are used.
Practice 4	Decisions concerning security aspects made by those empowered to make them are supported by others in the organization. TIP: • Ensure that necessary coordination of decisions with relevant all the people involved occurs.
Practice 5	Defined mechanisms are used for resolving conflicts and disputes referring to cybersecurity events TIP • Define the different types of conflicts that could appear: Scheduling difficulties, conflicts among commitments, budget or other financial issues, coordination problems • To resolve problems, issues, conflicts, or disputes take into account the knowledge and opinion of the individuals that their job is affected. • Communicate to all people involved the results of conflict and dispute resolution processes
Practice 6	Managers review the Participatory Culture activities status and results.
Practice 7	Measurements are made and used to determine the status and performance of Participatory Culture activities. TIP: Examples of measurements include the following: • Amount of business information communicated to the workforce • Number of conflict or dispute resolutions • Results from opinion feedback mechanisms. • Etc.

5 Cybersecurity Competency Model

A competency model can be defined as a framework that defines a set of knowledge, skill and abilities required to perform a specific job in a company. Competency models are widely used in business for defining and assessing competencies within organizations and supporting personnel managers in certain processes like staffing, recruiting or promoting.

In an energy company, the definition of the competency model is organised around the activity of the company, that is, energy generation, grid operation, energy services management, efficient consumption, etc. However, the increased digitization in the sector forces the workforce to acquire cybersecurity knowledge and skills. These competences will allow the people to avoid unconscious errors, reduce external threats, and be able to face adverse events (attacks and incidents) or system failures. Therefore, the competency model should include cybersecurity competences (knowledge, skills and abilities) required for each work role.

In this section we focus on the specific cybersecurity knowledge, abilities and skill that will be required by the personnel in the energy sector. We will start with a revision of the existing competency models in the cybersecurity and ICT domain and continue with an analysis of which cybersecurity knowledge, skills and abilities are required in each user Roles defined in Section 3.

5.1 Revision of existing Competency Models

5.1.1 European e-Competency Framework (e-CF)

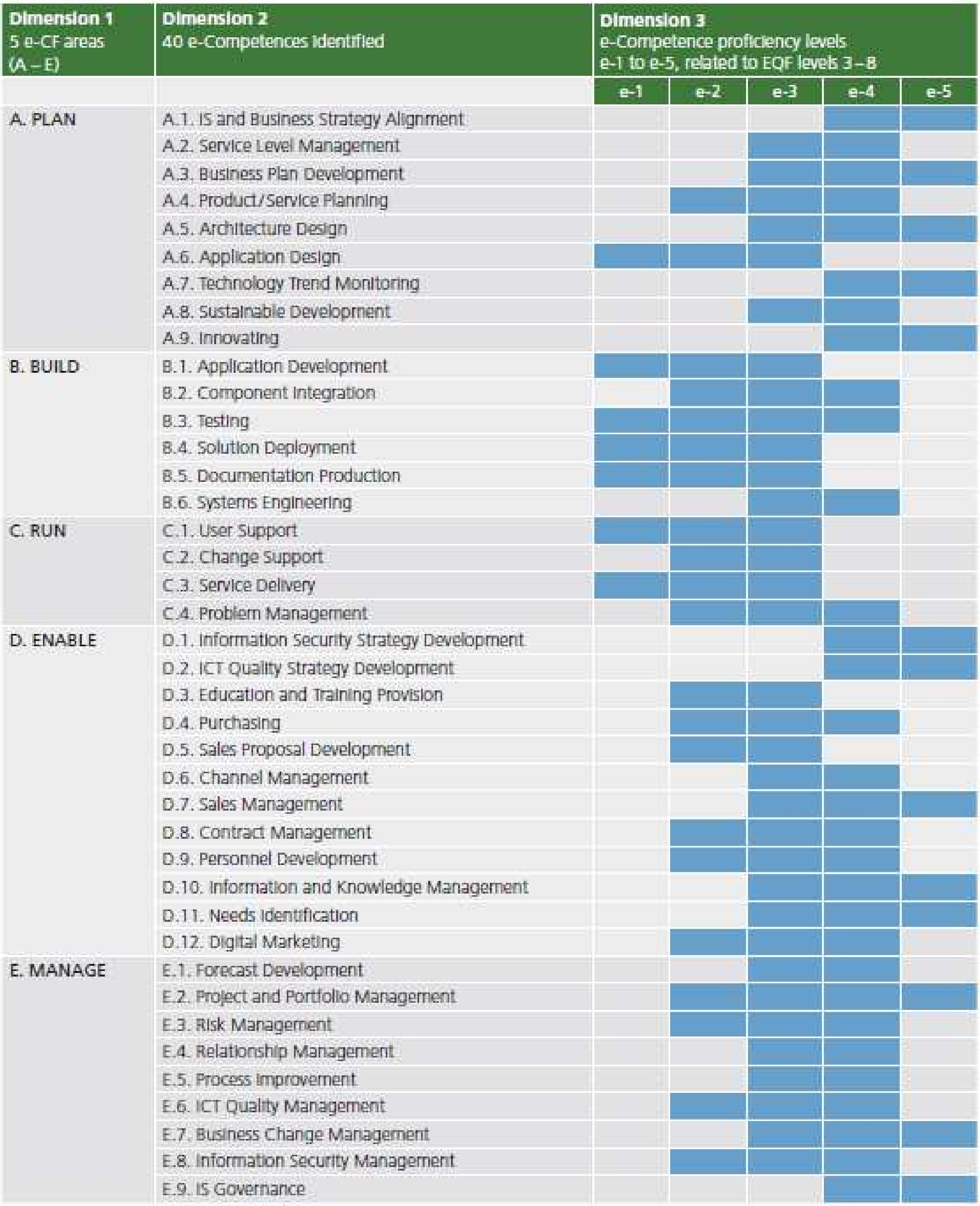
The European e-Competence Framework (e-CF) version 3.0[21] “*provides a reference of 40 competences as required and applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills and capability levels that can be understood across Europe, and that it implements of the European Qualifications Framework (EQF)*” [10].

The e-CF is structured over four dimensions. These dimensions reflect different levels of business and human resource planning requirements in addition to job/work proficiency guidelines. They are specified as follows:

- Dimension 1: The e-CF has 5 e-Competence areas, derived from the ICT business pro-cesses PLAN – BUILD – RUN – ENABLE – MANAGE.
- Dimension 2: A set of reference e-Competences for each area, with a generic description for each competence. 40 competences identified in total provide the European generic reference definitions of the framework.
- Dimension 3: Proficiency levels of each e-Competence provide European reference level specifications on e-Competence levels e-1 to e-5, which are related to EQF levels 3-8.
- Dimension 4: Samples of knowledge and skills relate to e-Competences in dimension 2. They are provided to add value and context and are not intended to be exhaustive.

[21] European qualifications framework (EQF). https://www.cedefop.europa.eu/es/events-and-projects/projects/european-qualifications-framework-eqf

Figure 18 shows the list of 40 e-Competences defined in e-CF.



Dimension 1 5 e-CF areas (A – E)	Dimension 2 40 e-Competences identified	Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3 – 8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment				■	■
	A.2. Service Level Management			■	■	
	A.3. Business Plan Development			■	■	■
	A.4. Product/Service Planning		■	■	■	
	A.5. Architecture Design			■	■	■
	A.6. Application Design	■	■	■		
	A.7. Technology Trend Monitoring				■	■
	A.8. Sustainable Development			■	■	
	A.9. Innovating				■	■
B. BUILD	B.1. Application Development	■	■	■		
	B.2. Component Integration		■	■	■	
	B.3. Testing	■	■	■	■	
	B.4. Solution Deployment	■	■	■		
	B.5. Documentation Production	■	■	■		
	B.6. Systems Engineering			■	■	
C. RUN	C.1. User Support	■	■	■		
	C.2. Change Support		■	■		
	C.3. Service Delivery	■	■	■		
	C.4. Problem Management		■	■	■	
D. ENABLE	D.1. Information Security Strategy Development				■	■
	D.2. ICT Quality Strategy Development				■	■
	D.3. Education and Training Provision		■	■		
	D.4. Purchasing		■	■	■	
	D.5. Sales Proposal Development		■	■		
	D.6. Channel Management			■	■	
	D.7. Sales Management			■	■	■
	D.8. Contract Management		■	■	■	
	D.9. Personnel Development		■	■	■	
	D.10. Information and Knowledge Management			■	■	■
	D.11. Needs Identification			■	■	■
	D.12. Digital Marketing		■	■	■	
E. MANAGE	E.1. Forecast Development			■	■	
	E.2. Project and Portfolio Management		■	■	■	■
	E.3. Risk Management		■	■	■	
	E.4. Relationship Management			■	■	
	E.5. Process Improvement			■	■	
	E.6. ICT Quality Management		■	■	■	
	E.7. Business Change Management			■	■	■
	E.8. Information Security Management		■	■	■	
	E.9. IS Governance				■	■

Figure 18. European e-Competency Framework (e-CF)

As far as security is concerned, e-CF lists two security related functions:

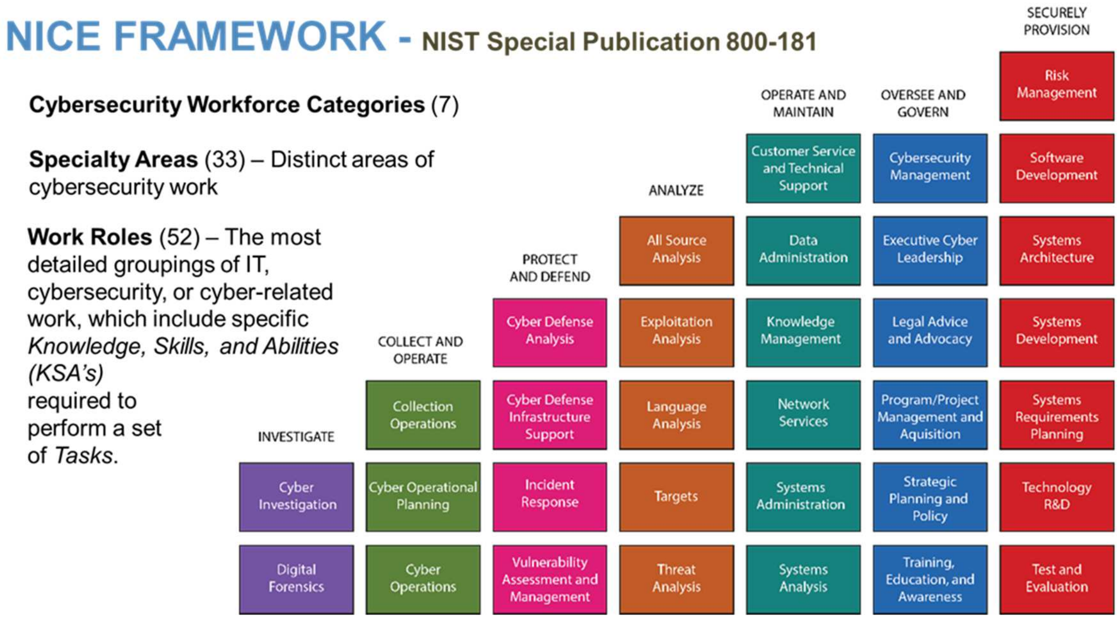
- **D.1. Information Security Strategy Development.** It defines and makes applicable a formal organisational strategy, scope and culture to maintain safety and security of information from external and internal threats, i.e. digital forensic for corporate investigations or intrusion investigation.
- **E.8. Information Security Management.** It implements information security policy. Monitors and takes action against intrusion, fraud and security breaches or leaks. Ensures that security risks are analysed and managed with respect to enterprise data and information. It reviews security incidents, makes recommendations for security policy and strategy to ensure continuous improvement of security provision.

5.1.2 NIST NICE

The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce has developed the NICE (National Initiative for Cybersecurity Education. The aim of the framework is to "*energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development*" [11]. NICE Framework is organised in:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role.

Figure 19 shows the work roles defined by NIST NICE.



NICE FRAMEWORK - NIST Special Publication 800-181

Cybersecurity Workforce Categories (7)

Specialty Areas (33) – Distinct areas of cybersecurity work

Work Roles (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific *Knowledge, Skills, and Abilities (KSA's)* required to perform a set of *Tasks*.

INVESTIGATE: Cyber Investigation; Digital Forensics

COLLECT AND OPERATE: Collection Operations; Cyber Operational Planning; Cyber Operations

PROTECT AND DEFEND: Cyber Defense Analysis; Cyber Defense Infrastructure Support; Incident Response; Vulnerability Assessment and Management

ANALYZE: All Source Analysis; Exploitation Analysis; Language Analysis; Targets; Threat Analysis

OPERATE AND MAINTAIN: Customer Service and Technical Support; Data Administration; Knowledge Management; Network Services; Systems Administration; Systems Analysis

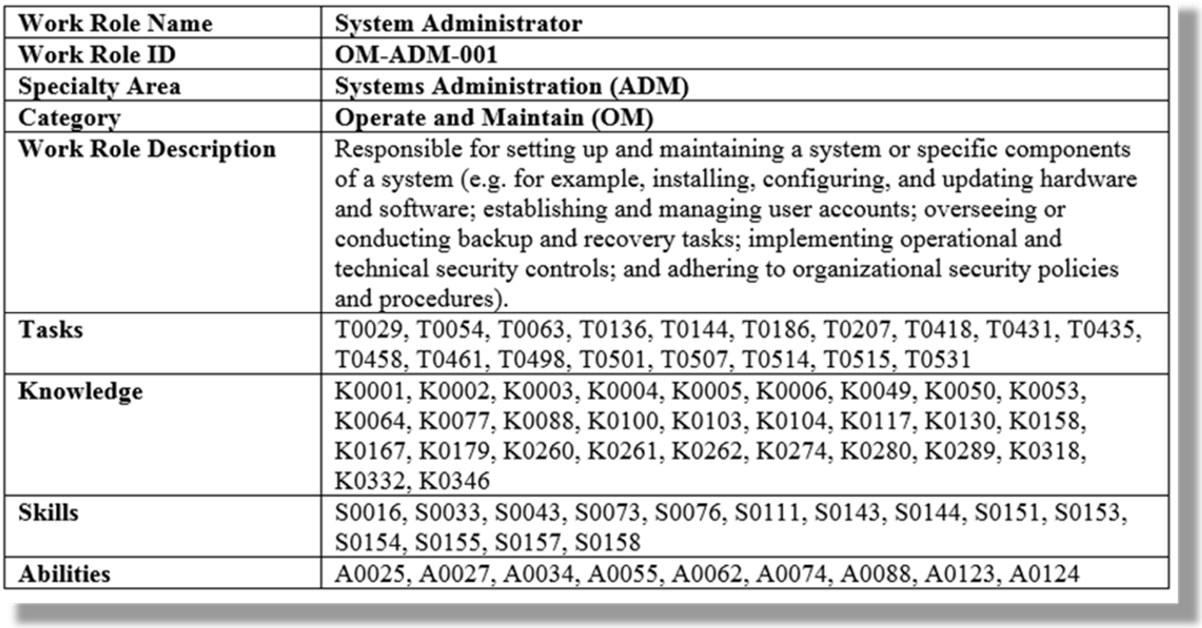
OVERSEE AND GOVERN: Cybersecurity Management; Executive Cyber Leadership; Legal Advice and Advocacy; Program/Project Management and Aquisition; Strategic Planning and Policy; Training, Education, and Awareness

SECURELY PROVISION: Risk Management; Software Development; Systems Architecture; Systems Development; Systems Requirements Planning; Technology R&D; Test and Evaluation

Figure 19. NIST NICE Work Roles

For each work role a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role has been defined. The framework defines 1007 tasks, 630 knowledges, 374 skills and 176 abilities.

Figure 20 shows an example of the information provided by NIST NICE Framework for the Database Administrator Work Role.



Work Role Name	**System Administrator**
Work Role ID	**OM-ADM-001**
Specialty Area	**Systems Administration (ADM)**
Category	**Operate and Maintain (OM)**
Work Role Description	Responsible for setting up and maintaining a system or specific components of a system (e.g. for example, installing, configuring, and updating hardware and software; establishing and managing user accounts; overseeing or conducting backup and recovery tasks; implementing operational and technical security controls; and adhering to organizational security policies and procedures).
Tasks	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346
Skills	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
Abilities	A0025, A0027, A0034, A0055, A0062, A0074, A0088, A0123, A0124

Figure 20. NIST NICE. System Administrator Work Role

Although some Work Roles are be very specific of the cybersecurity activities in a company (e.g., cyber investigation, threat analysis, collection operations, digital forensic), NIST NICE Framework provides very useful information for the definition of cybersecurity competences that should be incorporated by the personnel in an energy company.

We consider the NIST NICE Framework an important input for the elaboration of the SDN-microSENSE Cybersecurity Competency Model. However, there are many NICE roles that do not exist in energy companies and that cannot be easily matched against the roles defined in Section 3. Instead of matching NICE Work Roles we have decided to analyse NICE's knowledge, skills and abilities, classify them into set of Categories and Subcategories, and finally assign these categories and subcategories to our User Roles. The results of this work are presented in the following sections.

5.2 Cybersecurity Knowledge, Skills and Abilities (KSA)

NICE Framework defines knowledge, skills and abilities as "*the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training*" [11].

- **Knowledge** is a body of information applied directly to the performance of a function.
- **Skill** is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or

instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual.

- **Ability** is competence to perform an observable behaviour.

Starting from the list of knowledge, skills and abilities defined by the NICE Framework, and with the help of the SDN-microSENSE partners, a selection of the more significant knowledge, skills and abilities for each User Role defined in Section 3 has been done. The process followed, shown in Figure 21, has been the following:

1. Analysis of the NICE knowledge table and definition of a set of Categories and Subcategories.
2. Classification of each KSA into one Category and Subcategory.
3. Assignment of each Category and Subcategory to an SDN-microSENSE User Role.
4. Filter those KSA with limited impact of company security.

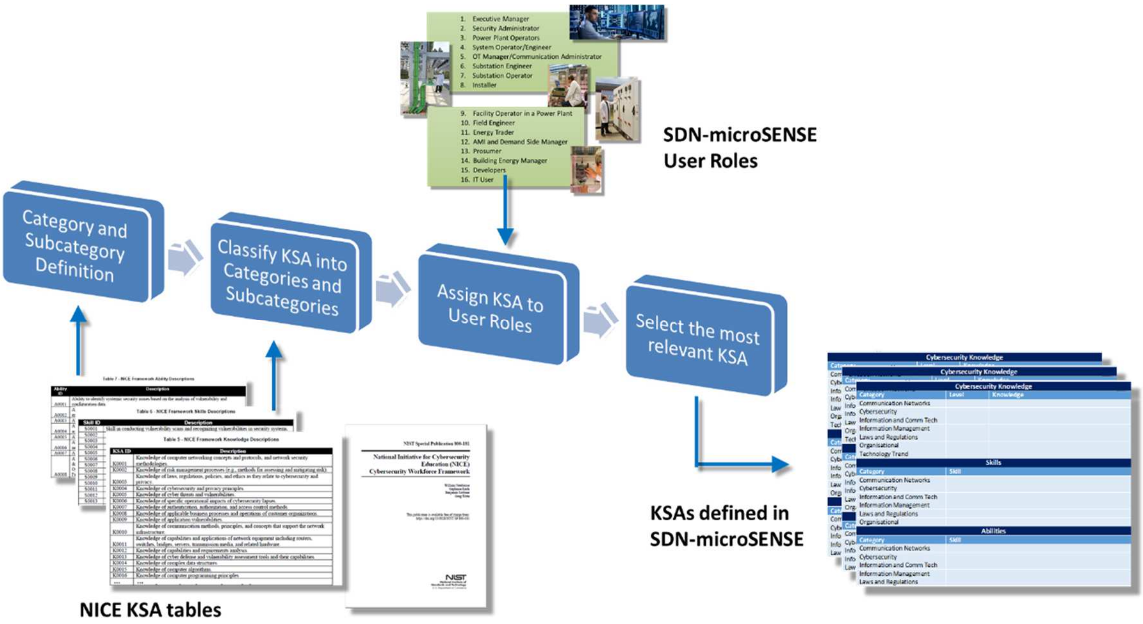

1. Executive Manager
2. Security Administrator
3. Power Plant Operators
4. System Operator/Engineer
5. OT Manager/Communication Administrator
6. Substation Engineer
7. Substation Operator
8. Installer
9. Facility Operator in a Power Plant
10. Field Engineer
11. Energy Trader
12. AMI and Demand Side Manager
13. Prosumer
14. Building Energy Manager
15. Developers
16. IT User
SDN-microSENSE User Roles
Category and Subcategory Definition
Classify KSA into Categories and Subcategories
Assign KSA to User Roles
Select the most relevant KSA
KSAs defined in SDN-microSENSE
NICE KSA tables
Cybersecurity Knowledge
Skills
Abilities

Figure 21. Selection of knowledge, skills and abilities for each User Role

5.3 Knowledge

This section provides the results of the analysis of cybersecurity knowledge required for each User Role:

- Table 22 lists the knowledge categories and subcategories and provides some example about the knowledge in each subcategory.
- Table 23 identifies which knowledge categories and subcategory are assigned to each user role and the level of knowledge required:
    - B = Basic knowledge

  - M = Medium knowledge
  - A = Advanced knowledge.
- The final set of knowledge for each role is provided in Annex I.

The following six knowledge are considered common to all roles by NICE Framework

- K0001. Knowledge of computer networking concepts and protocols, and network security methodologies.
- K0002. Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0003. Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0004. Knowledge of cybersecurity and privacy principles.
- K0005. Knowledge of cyber threats and vulnerabilities.
- K0006. Knowledge of specific operational impacts of cybersecurity lapses.

Table 22. Knowledge Categories and Subcategories

Collection	
Collection Management	Knowledge of collection management processes, capabilities, and limitations.
Collection Process	Knowledge of collection disciplines and capabilities.
Collection Tools	Knowledge of the available tools and applications associated with collection requirements and collection management.
Network and Communications	
Communication Fundamentals	Basic knowledge about networks and communications: • networking concepts and protocols. • telecommunications concepts. • basic computer components of a network, types of networks, etc. • Internet communications fundamentals.
Communication Technology	Advanced knowledge about a communication technology: • Bluetooth, RFID, IR, Wi-Fi, paging, cellular, satellite dishes, VoIP, etc. • structure, architecture, and design of modern wireless communications systems. • mobile cellular communications architecture.
Network Architectures	Knowledge of the basic structure, architecture, and design of modern communication networks: • physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc. • network architecture concepts including topology, protocols, and components. • how traffic flows across the network. • demilitarized zones. • organization's Local and Wide Area Network connections.
Network Management	Knowledge on network management: • network traffic analysis methods.

	• packet-level analysis: Wireshark, tcpdump, etc. • network tools: ping, traceroute, nslookup, etc. • network administration
Network Protocols	Knowledge about industrial and TCP/IP protocols: • OSI model. • network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services. • Internet and routing protocols.
Network Security	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware. • Virtual Private Network (VPN) security. • network security implementations: host-based IDS, IPS, access control lists. • basics of network security: encryption, firewalls, authentication, honey pots, perimeter protection.
ICT	
Database	Knowledge of database management systems, query languages, table relationships, and views: • Database systems. • database access application programming interfaces. • database administration and maintenance.
Hardware	Knowledge about the design and development of hardware devices: • microprocessors. • circuit analysis. • computer architectures.
IT Architectures	Knowledge of information technology (IT) architectural concepts and frameworks.
IT Systems	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly. • server administration and systems engineering theories, concepts, and methods. • systems administration concepts. • systems diagnostic tools and fault identification techniques. • file system implementations. • middleware. • principles and methods for integrating system components. • Supervisory control and data acquisition (SCADA).
Media Storage Devices	Knowledge of the characteristics of physical and virtual data storage media: • access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.
Operating Systems	Knowledge of operating systems:

	• server and client operating systems. • command-line tools: mkdir, mv, ls, passwd, grep, etc. • virtualization technologies and virtual machine development and maintenance. • system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems. • security concepts in operating systems.
Programming	Knowledge of computer programming principles: • programming concepts, including computer languages, programming, testing, debugging, and file types. • programming concepts: levels, structures, compiled vs. interpreted languages. • programming language structures and logic. • software debugging principles. • secure coding techniques. • Scripting. • embedded systems.
Software Development	Knowledge of software design tools, methods, and techniques: • software development models (e.g., Waterfall Model, Spiral Model). • software engineering. • software quality assurance process. • software reverse engineering techniques. • secure software deployment methodologies, tools, and practices. • configuration management techniques.
System Engineering	Knowledge of systems engineering theories, concepts, and methods.
Web Applications	Knowledge of how Internet applications work • SMTP email, web-based email, chat clients, VOIP, etc. • concepts related to websites: web servers/pages, hosting, DNS, registration, web languages such as HTML. • website types, administration, functions, and content management system (CMS). • web services: service-oriented architecture, Simple Object Access Protocol, and web service description language.
Information management	
Asset Management	Knowledge of sources, characteristics, and uses of the organization's data assets: • asset availability, capabilities and limitations. • hardware asset management. • software asset management. • patching and software updates.
Data Management	Knowledge of data administration and data standardization policies: • complex data structures. • data classification standards. • enterprise-wide information management.

	• information environment.
Data Processing	Knowledge of the capabilities and functionality associated with content creation and processing technologies: • wikis, social networking, content management systems, blogs. • taxonomy and semantic ontology theory. • how to utilize Hadoop, Java, Python, SQL, Hive, and Pig to explore data. • media production, communication, and dissemination techniques and methods. • methods, procedures, and techniques of gathering information and producing, reporting, and sharing information. • how to extract, analyze, and use metadata.
Data Security	Knowledge of critical information technology: • advanced data remediation security features in databases. • critical information requirements. • secure update mechanisms.
Law and Regulations	
Law and Regulations	Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures: • digital rights management. • electronic evidence law. • judicial process, including the presentation of facts and evidence. • cyber laws and their effect on Cyber planning. • privacy disclosure statements based on current laws.
Organisational Procedures and Company Policies	
Customer and Partners	Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information.
Deconfliction	Knowledge of deconfliction processes and procedures.
Human Resources	Knowledge of organizational human resource policies, processes, and procedures.
Intelligence	Knowledge of intelligence disciplines.
Learning Process	Knowledge of training and education policies, processes, and procedures: • instructional design and evaluation models. • learning assessment techniques. • computer based training and e-learning services. • Learning Management Systems and their use in managing learning • modes of learning. • training and education principles and methods for curriculum design.
Maturity Models	Knowledge of organizational process improvement concepts and process maturity models: • Capability Maturity Model Integration (CMMI). • measures or indicators of system performance and availability.
Organisation Policy and Procedures	• organizational planning and staffing process. • organization, roles and responsibilities. • organizational structure.

	• internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.
Security Policies	Knowledge of organizational security policies: • cyber operation objectives, policies, and legalities.
Security	
Access Control	Knowledge of authentication, authorization, and access control methods: • host/network access control mechanisms • network access, identity, and access management: public key infrastructure, Oauth, OpenID, SAML, SPML • developing and applying user credential management system • Unix and Windows systems that provide radius authentication and logging
Cyber Attacks	Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities: • adversarial tactics, techniques, and procedures • hacking methodologies • social dynamics of computer attackers in a global context • different classes of attacks: passive, active, insider, close-in, distribution attacks • cyber-attack stages: reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks • common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.) • denial and deception techniques. • structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques: gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network
Cyber Defense	Knowledge of cyber defense and information security policies, procedures, and regulations: • intrusion detection methodologies and techniques • system administration, network, and operating system hardening techniques. • security architecture concepts • application firewall concepts and functions • security models: Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model • software and methodologies for active defense and system hardening.
Encryption	Knowledge of cryptography and cryptographic key management concepts: encryption algorithms and methodologies
Ethical Hacking	Knowledge of ethical hacking principles and techniques: • hacking methodologies • penetration testing principles, tools, and technique

	• cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
Forensic Analysis	Knowledge of concepts and practices of processing digital forensic data: • which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files. • concepts and practices of processing digital forensic data.
Incident Reporting and Management	Knowledge of incident categories and incident responses: • incident response and handling methodologies. • target estimated repair and recuperation times. • enterprise incident response program, roles, and responsibilities. • crisis management protocols, processes, and techniques.
Intrusion and Malware Detection	Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization: • malware analysis tools: Oily Debug, Ida Pro • malware with virtual machine detection • physical and physiological behaviors that may indicate suspicious or abnormal activity • malware analysis concepts and methodologies. • Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
Risk Management	Knowledge of risk management processes: • methods for assessing and mitigating risk • Risk Management Framework • countermeasures for identified security risks. • risk scoring • risk assessment methodologies.
Security Fundamentals	Knowledge of cybersecurity and privacy principles: • Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • information security systems engineering principles • information technology (IT) security principles and methods • key concepts in security management • defense-in-depth principles and network security architecture • emerging security issues, risks, and vulnerabilities. • security management. • cyber lexicon/terminology • current and emerging cyber technologies.
Threat & Vulnerabilities	Knowledge of cyber threats and vulnerabilities: • vulnerability information dissemination sources • current and emerging threats/threat vectors. • risk/threat assessment. • cyber threat actors and their equities. • ways in which targets or threats use the Internet. •

Technology Trends	
Computer Algorithms	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics,
Machine Learning	Knowledge of machine learning theory and principles: • data mining and data warehousing principles • language processing tools and techniques
Technology Trends & Application	Knowledge of emerging technologies that have potential for exploitation

Table 23. Assignment of Knowledge Categories and Subcategory to EPES User Roles.

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Collection																	
Collection	Collection Management			B					M	B					A		B
	Collection Process		M	B				B	B	B	B			B	A	B	B
	Collection Tools		M				B		B	B	B				A		B
Communication Networks																	
Communication Networks	Communication Fundamentals	B	A	B	M	B	B	B	M	A	M	B	M	B	M	M	B
	Communication Technology		M			B				M	B		M			M	B
	Network Architectures	B	M	B	M	M				A	A		A			M	
	Network Management		M		M	B				M	A		M			A	
	Network Protocols		A	B	M	B	B	B	B	M	A		M			A	
	Network Security	B	A	B		B		B		M	M		M			A	
Information and Communication Technologies																	
Information and Communication Technologies	Database		M	B			B	B	M	B	B		M			A	B
	Hardware		M	B	M	B			M	B	B		M	M	A	B	
	IT Architectures		M	B	M					B	B		M			B	
	IT Systems		A	B	M		B	B	B	M	B	B	M	B	B	B	
	Media Storage Devices		M	B		M		B		A	B		A			B	
	Operating Systems		M	B	M			B	B	B	B		M	B	B	B	
	Programming		B							B	B		A			A	

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	Software Development		B							B	B		M			A	
	System Engineering		M	B	M		B			M	A	B					
	Web Applications		M					B		B			B			A	
Information Management																	
Information Management	Asset Management	A	A	B	M	A	B	B	M	A	B	M	B	M	B		B
	Data Management		M	B			B	B	M	M	B	B	B		M	M	B
	Data Processing		B	B				B	B	B	M	B	B		B	B	
	Data Security		A	B					B	B			B	B	B		
Law and Regulations																	
Law and Regulations	Law and Regulations	M	M	B			B	B	B	B	B	B	B		B		B
Organisational procedures and Company Policies																	
Organisational Procedures and Company Policies	Customer and Partners	A		B						A	B						B
	Deconfliction	A					B		B		B						
	Human Resources	A					B			B		B			B		B
	Intelligence			B											M		B
	Learning Process	M		B						B	B					B	
	Maturity Models	A	M	B					B	A					B		B
	Organisation Policy and Procedures	A	M	B			B	B		B	B	B			B	B	B
	Security Policies	B	A	B			B	B		B	B	B				B	
	Targeting and Tasking	A		B						B							B

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
									Security								
Security	Access Control		A	B		B	B	B	A	M	M	B	B	M	A	M	B
	Cyber Attacks		A	B		M		B	B	B	B		B			B	
	Cyber Defense		A	B		B	B	B		B	B		B			B	
	Encryption		M							B			B			B	
	Ethical Hacking		A	B		B				B	B		B			M	
	Forensic Analysis		A							B	B		B	B		B	
	Incident Reporting and Management		A	A		M	A	B	M	A	M	B			B	B	
	Intrusion and Malware Detection		A	B				B		B	B		B	M		M	
	Risk Management	B	A	B		B		B		B			B	B			
	Security Fundamentals	B	A	B	B	B	B	B	B	B	B	B	B	B		B	
	Threat & Vulnerabilities		A	B	B	B	B	B		B	B	B	B	B		B	
									Technology Trends								
Technology Trends	Computer Algorithms		B				B		B	B	B	B			B	B	B
	Machine Learning									B						B	B
	Technology Trends & Application	M	B	B		B	B		B	B	B	B			B		B

5.4 Skills

This section provides the result of the analysis of cybersecurity skills required for each User Role:

- Table 24 lists the skill categories and subcategories and provides some example about the skills in each subcategory.
- Table 25 identifies which skill categories and subcategory are assigned to each user role. In this case, different skill levels (Basic, Medium, Advanced) have not been considered.
- The final set of skills for each role is provided in Annex I.

Table 24. Knowledge Categories and Subcategories

Collection	
Collection Tools	• Skill to extract information from available tools and applications associated with collection operations management. • Skill to use collaborative tools and environments for collection operations.
Cybersecurity	
Access Control	• Skill in applying host/network access controls (e.g., access control list). • Skill in developing and applying security system access controls. • Skill in maintaining directory services.
Cyber Attacks	• Skill in the use of social engineering techniques. • Skill in recognizing and interpreting malicious network activity in traffic. • Skill in recognizing denial and deception techniques of the target.
Cyber Defense	• Skill in discerning the protection needs and evaluating the adequacy of security designs. • Skill in implementing and maintaining network security practices. • Skill in configuring and utilizing software-based protection tools. • Skill in protecting a network against malware. • Skill in applying security controls. • Skill in designing multi-level security/cross domain solutions. • Skill in system, network, and OS hardening techniques. • Skill in auditing firewalls, perimeters, routers, and intrusion detection systems. • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Encryption	• Skill in developing and deploying signatures and hash functions. • Skill in using Virtual Private Network (VPN) devices and encryption. • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications. • Skill in assessing the application of cryptographic standards. • Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.).
Ethical Hacking	• Skill in the use of penetration testing tools and techniques.
Forensic Analysis	• Skill in identifying and extracting data of forensic interest.

	• Skill in setting up a forensic workstation. • Skill in using forensic tool suites. • Skill in conducting forensic analyses in multiple environments. • Skill in deep analysis of captured malicious code. • Skill in reviewing logs to identify evidence of past intrusions.
Incident Reporting and Management	• Skill in using incident handling methodologies. • Skill in using security event correlation tools. • Skill in applying crisis planning procedures. • Skill to respond and take local actions in response to threat sharing alerts from service providers.
Intrusion and Malware Detection	• Skill in detecting host and network-based intrusions via intrusion detection technology. • Skill in analysing anomalous code as malicious or benign. • Skill in analysing malware. • Skill of identifying, capturing, containing, and reporting malware.
Risk Management	• Skill in designing countermeasures to identified security risks. • Skill in performing impact/risk assessments. • Skill to use risk scoring to help organizations to identify, assess, and manage cybersecurity risk.
Security Fundamentals	• Skill in applying confidentiality, integrity, and availability principles. • Skill in designing security controls based on cybersecurity principles. • Skill in applying security models.
Threat & Vulnerabilities	• Skill in recognizing and categorizing types of vulnerabilities and associated attacks. • Skill in using network analysis tools to identify vulnerabilities. • Skill in conducting application vulnerability assessments. • Skill in identifying cyber threats which may jeopardize organization and/or partner interests. • Skill in interpreting vulnerability scanner results to identify vulnerabilities. • Skill to anticipate new security threats.
Network and Communications	
Communication Technology	• Skill in survey, collection, and analysis of wireless LAN metadata. • Skill in using non-attributable networks. • Skill in wireless network target analysis, templating, and geolocation.
Network Architectures	• Skill in applying various subnet techniques. • Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks. • Skill in analysing traffic to identify network devices. • Skill in determining the physical location of network devices. • Skill in identifying a target’s communications networks. • Skill in identifying the devices that work at each level of protocol models. • Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction.

Network Management	• Skill in analysing network traffic capacity and performance characteristics. • Skill in diagnosing connectivity problems. • Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches. • Skill in using network management tools to analyse network traffic. • Skill in using protocol analysers. • Skill in network systems management principles, models, methods and tools. • Skill in extracting information from packet captures.
ICT	
Database	• Skill in generating queries and reports and using Boolean operators to construct simple and complex queries. • Skill in maintaining databases. • Skill in optimizing database performance.
Hardware	• Skill in tuning sensors. • Skill in physically disassembling PCs.
IT Systems	• Skill in designing the integration of hardware and software solutions. • Skill in identifying possible causes of degradation of system performance. • Skill in conducting system/server planning, management, and maintenance. • Skill in correcting physical and technical problems that impact system/server performance. • Skill in installing system and component upgrades. • Skill in monitoring and optimizing system/server performance. • Skill in recovering failed systems/servers. • Skill in determining installed patches on various operating systems and identifying patch signatures. • Skill in server administration.
Operating Systems	• Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux. • Skill in using virtual machines. • Skill in operating system administration.
Programming	• Skill in writing code in a currently supported programming language. • Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc. • Skill in interpreting compiled and interpretive programming languages. • Skill in remote command line and Graphic User Interface (GUI). • Skill in applying secure coding techniques. • Skill in conducting software debugging and interpreting results of debugger to ascertain tactics, techniques, and procedures.
Software Development	• Skill in writing and conducting test plans. • Skill in configuring and optimizing software. • Skill in design modelling and building use cases. • Skill in designing and documenting overall program Test & Evaluation strategies.

Information management	
Asset Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization's data assets.
Data Management	• Skill in using knowledge management technologies. • Skill in using multiple search engines and tools in conducting open-source searches.
Data Processing	• Skill in designing a data analysis structure. • Skill in developing data models and dictionaries. • Skill in data pre-processing and performing format conversions to create a standard representation of the data. • Skill in developing machine understandable semantic ontologies. • Skill in conducting social network analysis. • Skill in creating and extracting important information from packet captures. • Skill in evaluating and interpreting metadata. • Skill in using data analysis tools.
Law and Regulations	
Law and Regulations	• Skill in preserving evidence integrity according to standard operating procedures or national standards. • Skill in complying with the legal restrictions for targeted information.
Organisational Procedures and Company Policies	
Customer and Partners	• Skill in interfacing with customers. • Skill in managing client relationships. • Skill in negotiating vendor agreements and evaluating vendor privacy practices. • Skill to analyse and assess internal and external partner reporting.
Intelligence	• Skill in developing intelligence reports.
Organisation Policy and Procedures	• Skill in applying organization-specific systems analysis principles and techniques. • Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success.
Technology Trends	
Computer Algorithms	• Skill in creating and utilizing mathematical or statistical models. • Skill in using scientific rules and methods to solve problems.
Machine Learning	• Skill in data mining techniques.
Technology Trends & Application	• Skill to remain aware of evolving technical infrastructures.
Personal Skills	
Personal Skills	• Skill in preparing and presenting briefings. • Skill in preparing plans and related correspondence. • Skill in reviewing and editing plans. • Skill in writing effectiveness reports.

Table 25. Assignment of Skill Categories to EPES User Roles.

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Collection																	
Collection	Collection Management																
	Collection Process																
	Collection Tools	X						X									
Communication Networks																	
Communication Networks	Communication Technology									X			X			X	
	Network Architectures									X			X			X	
	Network Management									X			X			X	
Information and Communication Technologies																	
Information and Communication Technologies	Database	X	X	X	X	X	X	X	X	X	X	X	X		X	X	
	Hardware									X			X				
	IT Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Operating Systems									X			X			X	
	Programming															X	
	Software Development									X			X			X	
Information Management																	
Information Management	Asset Management	X	X	X	X	X	X	X	X	X	X	X	X		X		
	Data Management	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Data Processing	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Law and Regulations																	
Law and Regulations	Law and Regulations	X	X	X			X	X	X						X		
Organisational procedures and Company Policies																	
Organisational Procedures and Company Policies	Customer and Partners	X						X									
	Human Resources																
	Intelligence	X						X									
	Learning Process																
	Organisation Policy and Procedures	X	X	X			X	X	X						X		
Security																	
Security	Access Control		X							X							
	Cyber Attacks		X							X			X				
	Cyber Defense		X							X			X			X	
	Encryption									X			X			X	
	Ethical Hacking		X							X							
	Forensic Analysis		X							X							
	Incident Reporting and Management		X														
	Intrusion and Malware Detection		X							X							
	Risk Management	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Security Fundamentals	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Threat & Vulnerabilities		X							X							

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Technology Trends																	
Technology Trends	Computer Algorithms															X	
	Machine Learning															X	
	Technology Trends & Application		X							X						X	
Personal Skills																	
Personal Skills	Personal Skills	X	X	X			X	X	X								

5.5 Abilities

This section provides the result of the analysis of cybersecurity abilities required for each User Role:

- Table 26 lists the ability categories and subcategories and provides some example about the skills in each subcategory.
- Table 27 identifies which ability categories and subcategory are assigned to each user role. In this case, different ability levels (Basic, Medium, Advanced) have not been considered.
- The final set of abilities for each role is provided in Annex I.

Table 26. Knowledge Categories and Subcategories

Cybersecurity	
Cyber Attacks	• Ability to identify/describe techniques/methods for conducting technical exploitation of the target.
Cyber Defense	• Ability to prioritize and allocate cybersecurity resources correctly. • Ability to conduct a comprehensive assessment of the management, operational, and technical security controls. • Ability to assesses a security plan. • Ability to identify critical infrastructure systems.
Forensic Analysis	• Ability to conduct forensic analyses.
Incident Reporting and Management	• Ability to design incident response for cloud service models.
Intrusion and Malware Detection	• Ability to analyse malware. • Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
Risk Management	• Ability to apply supply chain risk management standards. • Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system. • Ability to recognize that changes to systems or environment can change residual risks.
Security Fundamentals	• Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance. • Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • Ability to conduct systems security engineering activities. • Ability to find and navigate the dark web using the TOR network to locate markets and forums.
Threat & Vulnerabilities	• Ability to conduct vulnerability scans and recognize vulnerabilities in security systems. • Ability to identify/describe target vulnerability.

Communication Networks	
Network Architectures	• Ability to apply network security architecture concepts including topology, protocols, components, and principles. • Ability to design and build architectures and frameworks. • Ability to set up physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks.
Network Management	• Ability to operate common network tools. • Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware • Ability to track the location and configuration of networked devices and software across departments, locations and facilities. • Ability to monitor traffic flows across the network. • Ability to perform network collection tactics, techniques, and procedures to include decryption capabilities/tools. • Ability to interpret the information collected by network tools.
Information and Communication Technologies	
Database	• Ability to maintain databases. (i.e., backup, restore, delete data, transaction log files, etc.).
IT Systems	• Ability to apply secure system design tools, methods and techniques. • Ability to monitor measures or indicators of system performance and availability. • Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). • Ability to integrate information security requirements into the acquisition process.
Operating Systems	• Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat). • Ability to examine digital media on multiple operating system.
Programming	• Ability to apply programming language structures and logic. • Ability to develop secure software according to secure software deployment methodologies, tools, and practices. • Ability to employ best practices when implementing security controls.
Software Development	• Ability to capture and refine security requirements and ensure that are effectively integrated into the component products and systems. • Ability to collect, verify, and validate test data. • Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools. • Ability to execute technology integration processes. • Ability to interpret and translate customer requirements into operational capabilities.
Information management	
Data Security	• Ability to ensure information security management processes are integrated with strategic and operational planning processes. • Ability to establish the rules for appropriate use and protection of the information.
Data Processing	• Ability to decrypt digital data collections. • Ability to translate data and test results into evaluative conclusions.

	• Ability to use data visualization tools. • Ability to evaluate information for reliability, validity, and relevance. • Ability to evaluate, analyse, and synthesize large quantities of data.
Law and Regulations	
Law and Regulations	• Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action. • Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies. • Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives. • Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance. • Ability to author a privacy disclosure statement based on current laws.
Organisational Procedures and Company Policies	
Customer and Partners	• Ability to evaluate the trustworthiness of the supplier and/or product. • Ability to identify external partners with common cyber operations interests. • Ability to interpret and translate customer requirements. • Ability to tailor technical and planning information to a customer's level of understanding. • Ability to ensure that functional and security requirements are appropriately addressed in a contract.
Human Resources	• Ability to assess and forecast manpower requirements to meet organizational objectives. • Ability to determine the validity of workforce trend data. • Ability to apply approved planning development and staffing processes.
Learning Process	• Ability to prepare and deliver education and awareness briefings. • Ability to gauge learner understanding and knowledge level. • Ability to provide effective feedback to students for improving learning. • Ability to apply principles of adult learning. • Ability to develop clear directions and instructional materials. • Ability to develop curriculum for use within a virtual environment. • Ability to apply the Instructional System Design (ISD) methodology. • Ability to conduct training and education needs assessment.
Intelligence	• Ability to identify intelligence gaps. • Ability to utilize multiple intelligence sources across all intelligence disciplines.
Security Policies	• Ability to develop policy, plans, and strategy in compliance with laws, regulations, and standards in support of organizational cyber activities. • Ability to work across departments and business units to implement organization's privacy principles align with security objectives.
Organisation Policy and Procedures	• Ability to coordinate cyber operations with other organization functions or support activities. • Ability to coordinate, collaborate and disseminate information to subordinate, lateral and higher-level organizations.

	• Ability to ensure the organization has adequately trained personnel to assist in complying with security requirements in legislation, Executive Orders, policies, directives, instructions, standards, and guidelines. • Ability to coordinate with senior leadership of an organization to develop a risk management strategy for the organization. • Ability to work closely with authorizing officials to help ensure that security considerations are integrated.
Technology Trends	
Computer Algorithms	• Ability to use and understand complex mathematical concept. • Ability to interpret and understand complex and rapidly evolving concepts. • Ability to design capabilities to find solutions to less common and more complex system problems.
Machine Learning	• Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
Technology Trends & Application	• Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues. • Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
Personal Skills	
Personal Skills	• Ability to answer questions in a clear and concise manner. • Ability to ask clarifying questions. • Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner. • Ability to facilitate small group discussions. • Ability to prepare and present briefings and produce technical documentation. • Ability to design valid and reliable assessments. • Ability to apply critical reading/thinking skills. • Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts to leverage analytical and technical expertise. • Ability to think critically. • Ability to understand objectives and effects. • Ability to recognize and mitigate deception in reporting and analysis

Table 27. Assignment of Knowledge Categories and Subcategory to EPES User Roles.

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Communication Networks																	
Communication Networks	Network Architectures									X			X			X	
	Network Management									X			X			X	
Information and Communication Technologies																	
Information and Communication Technologies	Database															X	
	IT Systems	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Operating Systems									X			X			X	
	Programming															X	
	Software Development															X	
Information Management																	
Information Management	Data Processing	X	X	X		X	X	X	X	X	X		X		X	X	
	Data Security	X	X														
Law and Regulations																	
Law and Regulations	Law and Regulations	X	X					X							X		
Organisational procedures and Company Policies																	
Organisational Procedures and Company Policies	Customer and Partners	X															
	Human Resources	X															
	Intelligence	X															
	Organisation Policy and Procedures	X	X														

		Executive Manager	Security Admin	Power Plant Oper.	Facility Oper. (PP)	Field Engineer	System Oper. / Engineer	Energy Trader	AMI and DSM	OT Manager / Comm. Admin	Subst. Engineer	Subst. Operator	Installer	Prosumer	Building EM	Developers	IT User
Knowledge Category	**Knowledge Subcategory**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	Security Policies	X	X					X									
Security																	
Security	Cyber Attacks		X														
	Cyber Defense		X			X					X						
	Forensic Analysis		X														
	Incident Reporting and Management		X														
	Intrusion and Malware Detection																
	Risk Management		X			X				X	X						
	Security Fundamentals	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Threat & Vulnerabilities									X							
Technology Trends																	
Technology Trends	Computer Algorithms																
	Machine Learning																
	Technology Trends & Application																
Personal Skills																	
Personal Skills	Personal Skills	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

6 Evaluation Tool

The objective of the Evaluation Tool is to measure the Maturity Level of an Energy Company regarding the Cybersecurity Awareness Maturity Model described in Section 4.

This tool, developed in EXCEL, helps a company to assess which processes have been deployed satisfactorily, which have not been deployed and which have been deployed partially. With this information the tool elaborates a set of tables and graphs showing level of maturity of the company.

The tool contains the following elements:

1. Cover form. It provides general information of the tool: name, version, brief description, …
2. Evaluation summary form.
3. Level 2 (people managed) results presentation form.
4. Level 3 (competency managed) results presentation form.
5. Processes assessment form.

The following sections present the elements of the Evaluation Tool.

6.1 Colour Code

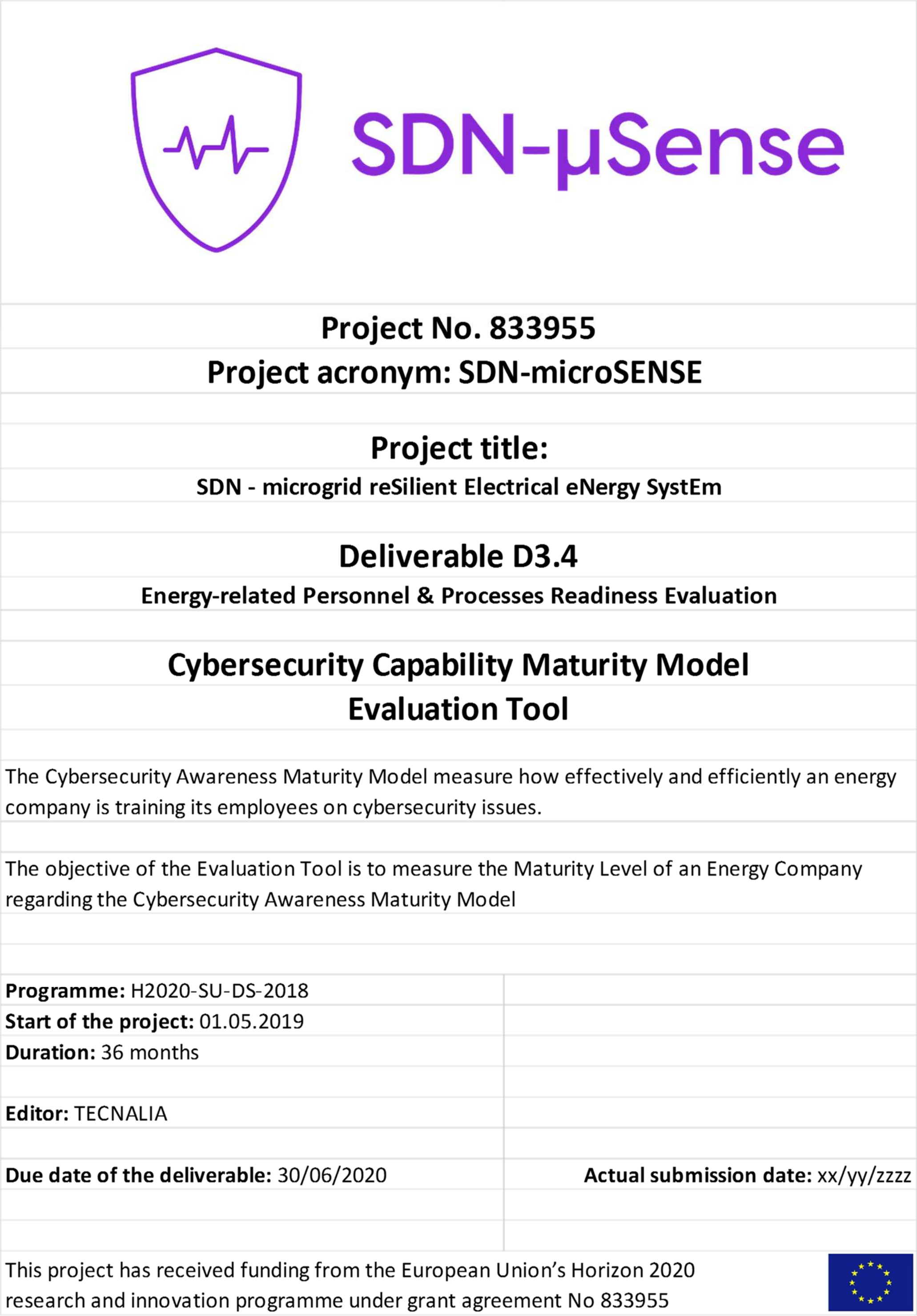
The evaluation tool uses a colour code to shows if a practice or a process has been totally satisfied (green) partially satisfied (yellow) or not satisfied (red) by the company. Table 28 provides a brief explanation of the colour meaning.

Table 28. Colour code used in the Evaluation Tool

Colour	Meaning
Red	The purpose of the practice is judged as absent or poorly addressed within the set of implemented practices - deficiencies or problems were identified that will impede the achievement of the goal in the case that the deployment is carried out in this way throughout the organizational unit.
Yellow	The purpose of the practice is judged as partially addressed within the set of practices implemented - deficiencies or problems that could threaten the achievement of the goal were identified in the case that the deployment was carried out in this way throughout the organizational unit
Green	The purpose of the practice is judged as adequately addressed within the set of implemented practices - in a way that would allow the goal to be met in the case that the practice was deployed throughout the organizational unit.
White	The practices are not applicable in the context of the organization.

6.2 Cover Form

It provides general information of the tool as it is shown in Figure 22.



Project No. 833955

Project acronym: SDN-microSENSE

Project title:

SDN - microgrid reSilient Electrical eNergy SystEm

Deliverable D3.4

Energy-related Personnel & Processes Readiness Evaluation

Cybersecurity Capability Maturity Model
Evaluation Tool

The Cybersecurity Awareness Maturity Model measure how effectively and efficiently an energy company is training its employees on cybersecurity issues.

The objective of the Evaluation Tool is to measure the Maturity Level of an Energy Company regarding the Cybersecurity Awareness Maturity Model

Programme: H2020-SU-DS-2018	
Start of the project: 01.05.2019	
Duration: 36 months	
Editor: TECNALIA	
Due date of the deliverable: 30/06/2020	**Actual submission date:** xx/yy/zzzz

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833955

Figure 22. Evaluation tool. Tool description form.

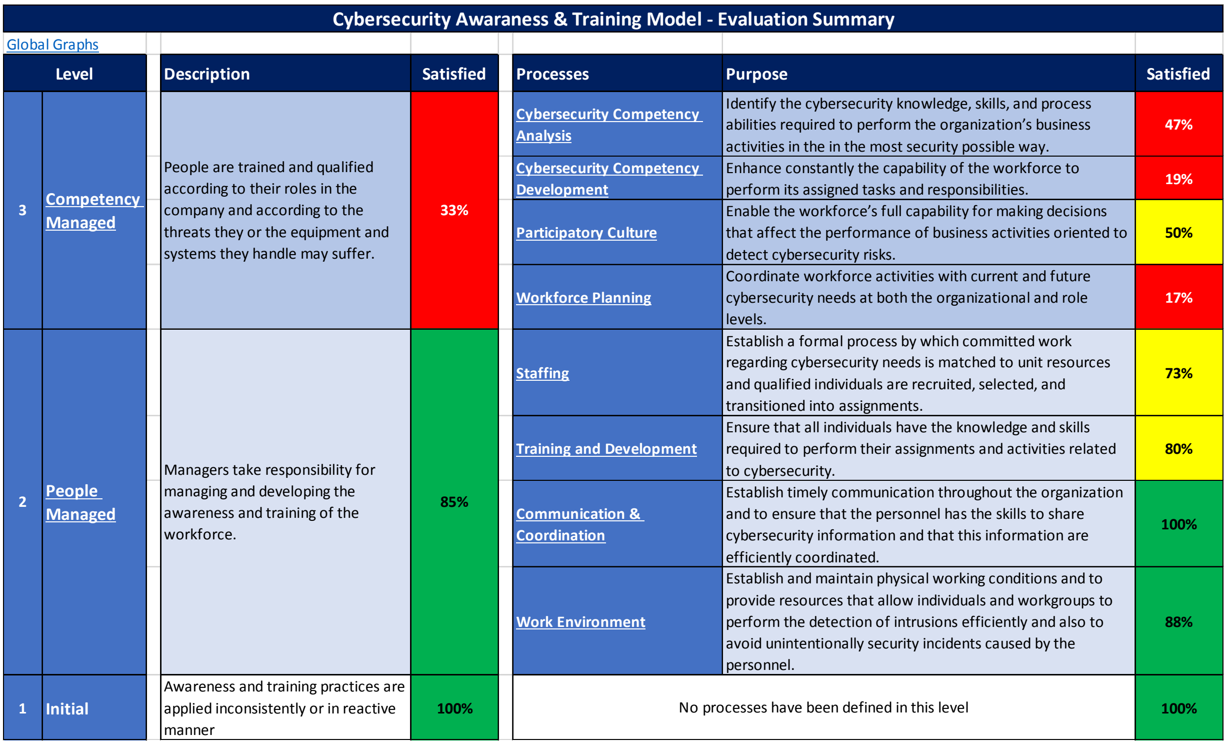
6.3 Evaluation Summary form

This form provides the summary of the whole evaluation process. The user can have a global idea about the level of deployment of the Cybersecurity Awareness & Training Model in the company.

The main elements of this form are the followings:

1. Model levels: provides a brief description of each level and the degree of development achieved by the company. You can click in the level name to go to the corresponding level form.
2. Process: Show a brief description of each process and the degree of development achieved by the company. You can click in the level name to go to the corresponding level form.

Figure 23 shows an example of the Evaluation Summary Form, where we can appreciate how level 2 (People Managed) has been satisfied (green colour) as all the processes of this level have been satisfied. On the contrary Workforce Planning process has not been satisfied at level 3 (Competency Managed) and the other three processes have been satisfied partially. Therefore, the Competence Managed Level is considered partially satisfied (yellow colour). This can be more clearly appreciated in Figure 24 and Figure 25.

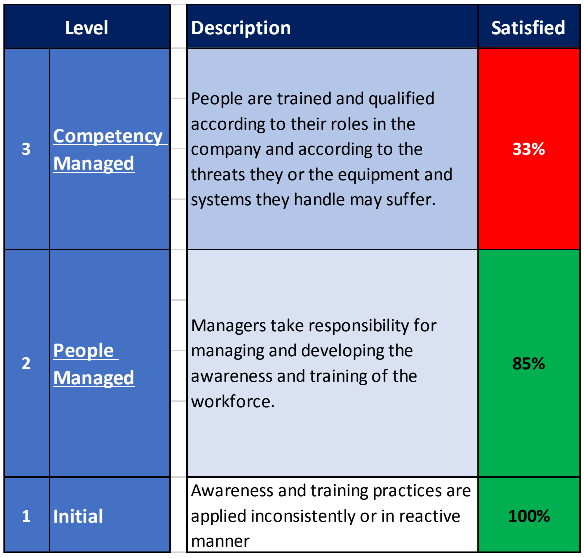


Cybersecurity Awareness & Training Model - Evaluation Summary

Global Graphs

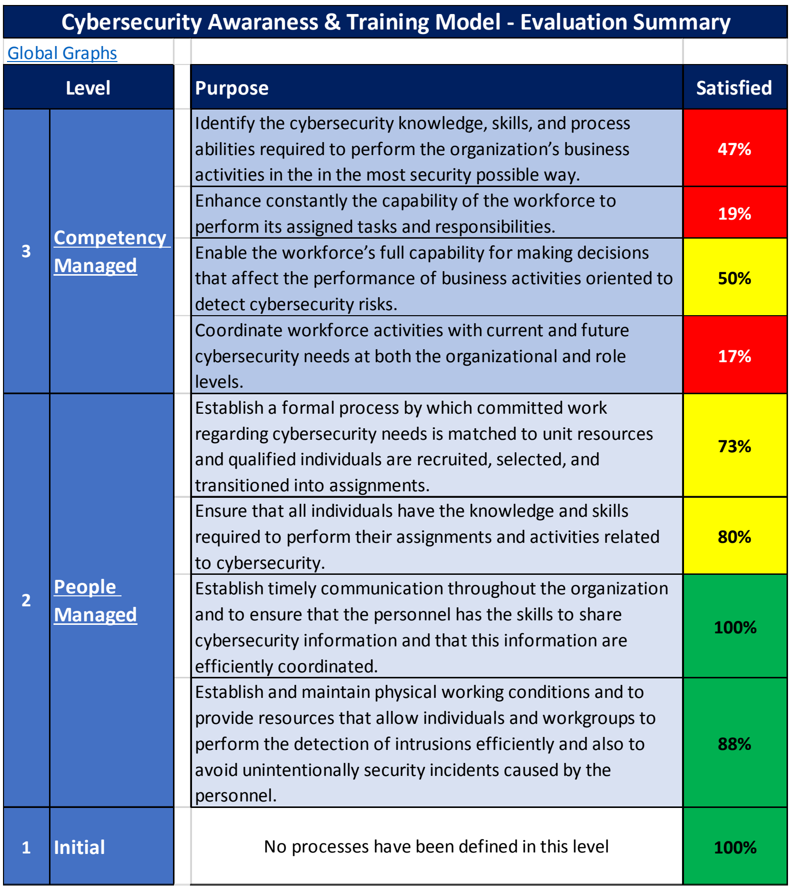
Level		Description	Satisfied	Processes	Purpose	Satisfied
3	Competency Managed	People are trained and qualified according to their roles in the company and according to the threats they or the equipment and systems they handle may suffer.	33%	Cybersecurity Competency Analysis	Identify the cybersecurity knowledge, skills, and process abilities required to perform the organization's business activities in the in the most security possible way.	47%
				Cybersecurity Competency Development	Enhance constantly the capability of the workforce to perform its assigned tasks and responsibilities.	19%
				Participatory Culture	Enable the workforce's full capability for making decisions that affect the performance of business activities oriented to detect cybersecurity risks.	50%
				Workforce Planning	Coordinate workforce activities with current and future cybersecurity needs at both the organizational and role levels.	17%
2	People Managed	Managers take responsibility for managing and developing the awareness and training of the workforce.	85%	Staffing	Establish a formal process by which committed work regarding cybersecurity needs is matched to unit resources and qualified individuals are recruited, selected, and transitioned into assignments.	73%
				Training and Development	Ensure that all individuals have the knowledge and skills required to perform their assignments and activities related to cybersecurity.	80%
				Communication & Coordination	Establish timely communication throughout the organization and to ensure that the personnel has the skills to share cybersecurity information and that this information are efficiently coordinated.	100%
				Work Environment	Establish and maintain physical working conditions and to provide resources that allow individuals and workgroups to perform the detection of intrusions efficiently and also to avoid unintentionally security incidents caused by the personnel.	88%
1	Initial	Awareness and training practices are applied inconsistently or in reactive manner	100%	No processes have been defined in this level		100%

Figure 23. Evaluation tool. Evaluation summary form.



Level		Description	Satisfied
3	Competency Managed	People are trained and qualified according to their roles in the company and according to the threats they or the equipment and systems they handle may suffer.	33%
2	People Managed	Managers take responsibility for managing and developing the awareness and training of the workforce.	85%
1	Initial	Awareness and training practices are applied inconsistently or in reactive manner	100%

Figure 24. Evaluation summary form. Compliance degree of each maturity level.



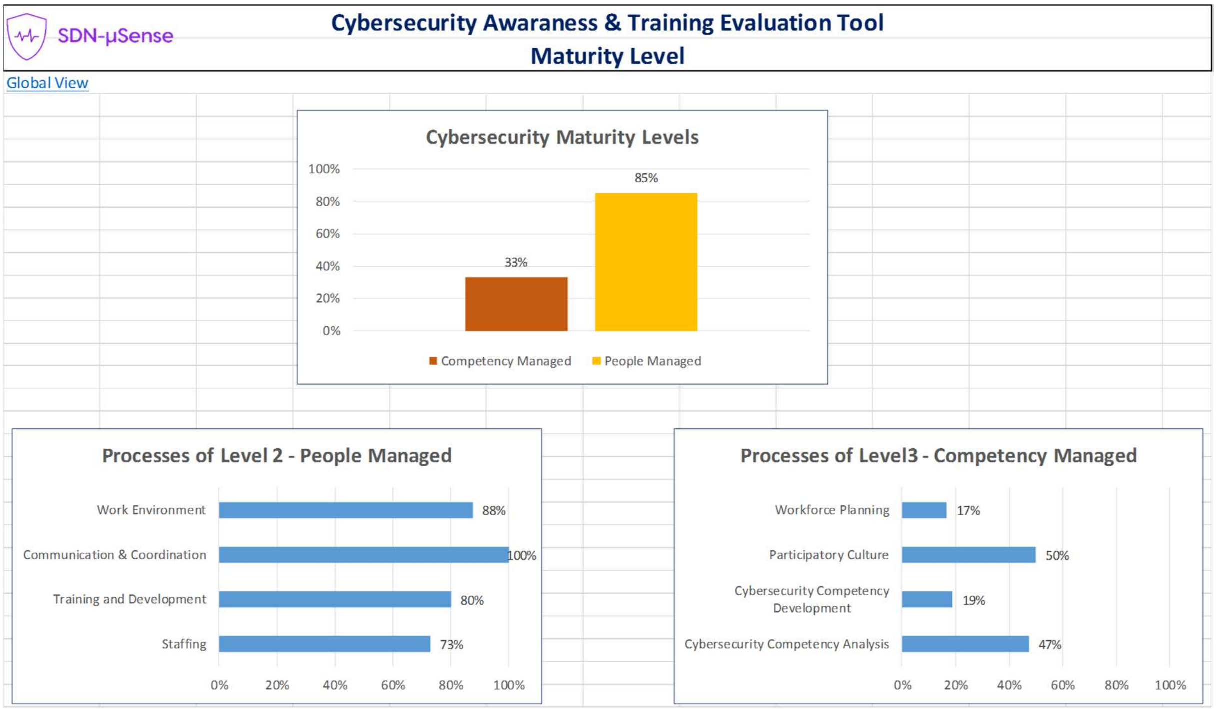
Cybersecurity Awaraness & Training Model - Evaluation Summary

Global Graphs

Level		Purpose	Satisfied
3	Competency Managed	Identify the cybersecurity knowledge, skills, and process abilities required to perform the organization's business activities in the in the most security possible way.	47%
		Enhance constantly the capability of the workforce to perform its assigned tasks and responsibilities.	19%
		Enable the workforce's full capability for making decisions that affect the performance of business activities oriented to detect cybersecurity risks.	50%
		Coordinate workforce activities with current and future cybersecurity needs at both the organizational and role levels.	17%
2	People Managed	Establish a formal process by which committed work regarding cybersecurity needs is matched to unit resources and qualified individuals are recruited, selected, and transitioned into assignments.	73%
		Ensure that all individuals have the knowledge and skills required to perform their assignments and activities related to cybersecurity.	80%
		Establish timely communication throughout the organization and to ensure that the personnel has the skills to share cybersecurity information and that this information are efficiently coordinated.	100%
		Establish and maintain physical working conditions and to provide resources that allow individuals and workgroups to perform the detection of intrusions efficiently and also to avoid unintentionally security incidents caused by the personnel.	88%
1	Initial	No processes have been defined in this level	100%

Figure 25. Evaluation summary form. Compliance degree of each process.

Figure 26

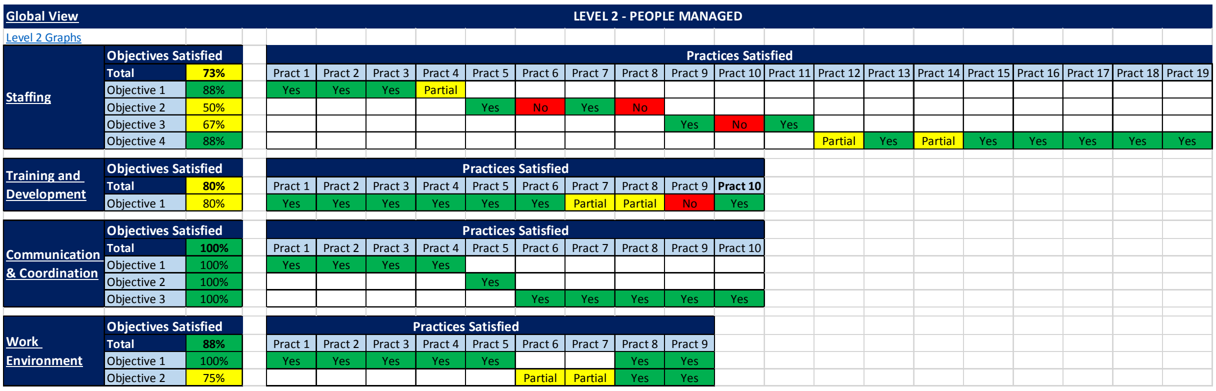

Cybersecurity Awareness & Training Evaluation Tool
Maturity Level

Global View

Figure 26. Evaluation tool. Statistical graphs

6.4 Level 2 Evaluation Summary Form

This form provides the summary of the Level 2 (People Managed) evaluation process. The user can have a global idea about the degree of deployment of the processes of the People Managed level. Figure 27 shows an example of the People Managed Level Summary Form.


Global View — LEVEL 2 - PEOPLE MANAGED

Level 2 Graphs

	Objectives Satisfied		Practices Satisfied																		
Staffing	Total	73%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	Pract 9	Pract 10	Pract 11	Pract 12	Pract 13	Pract 14	Pract 15	Pract 16	Pract 17	Pract 18	Pract 19
	Objective 1	88%	Yes	Yes	Yes	Partial															
	Objective 2	50%					Yes	No	Yes	No											
	Objective 3	67%									Yes	No	Yes								
	Objective 4	88%												Partial	Yes	Partial	Yes	Yes	Yes	Yes	Yes

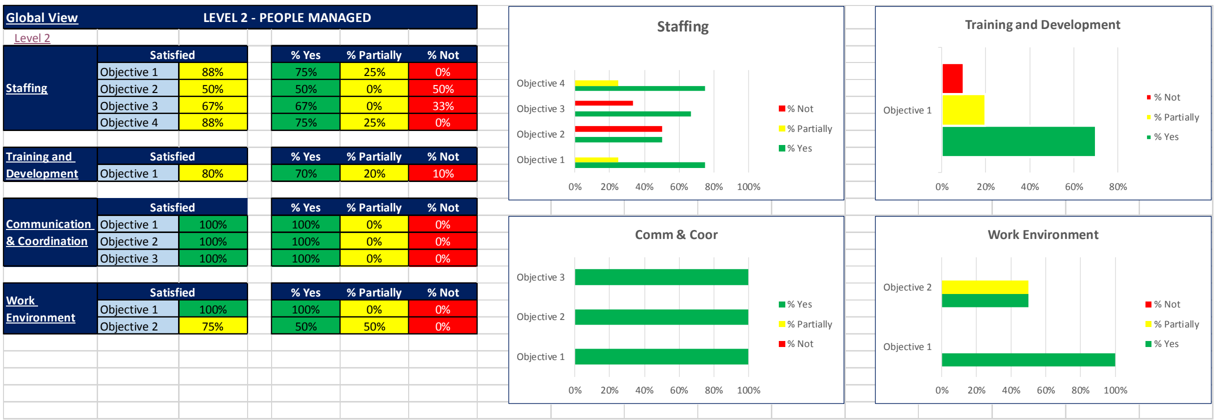
	Objectives Satisfied		Practices Satisfied									
Training and Development	Total	80%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	Pract 9	**Pract 10**
	Objective 1	80%	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Partial	No	Yes

	Objectives Satisfied		Practices Satisfied									
Communication & Coordination	Total	100%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	Pract 9	Pract 10
	Objective 1	100%	Yes	Yes	Yes	Yes						
	Objective 2	100%					Yes					
	Objective 3	100%						Yes	Yes	Yes	Yes	Yes

	Objectives Satisfied		Practices Satisfied								
Work Environment	Total	88%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	Pract 9
	Objective 1	100%	Yes	Yes	Yes	Yes	Yes			Yes	Yes
	Objective 2	75%						Partial	Partial	Yes	Yes

Figure 27. Evaluation tool. Level 2, People Managed, evaluation summary form.

Figure 28 shows the statistical graphs representing the percentage of achievement for each process of level 2, People Managed.

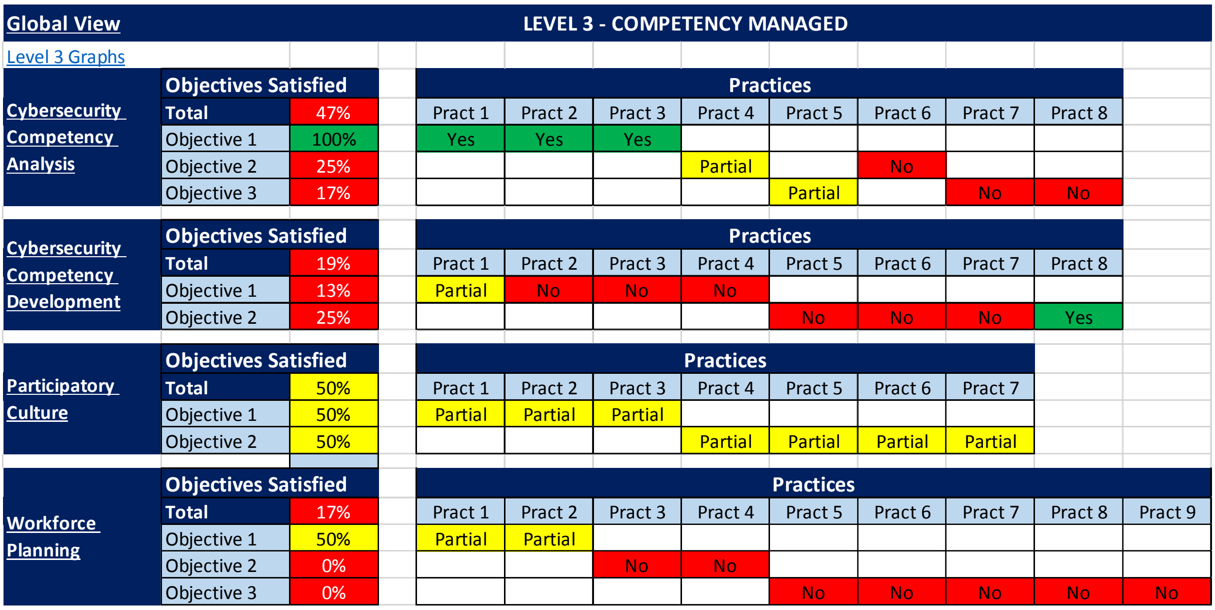


Global View	LEVEL 2 - PEOPLE MANAGED		% Yes	% Partially	% Not
Level 2					
Staffing	Satisfied		% Yes	% Partially	% Not
	Objective 1	88%	75%	25%	0%
	Objective 2	50%	50%	0%	50%
	Objective 3	67%	67%	0%	33%
	Objective 4	88%	75%	25%	0%
Training and Development	Satisfied		% Yes	% Partially	% Not
	Objective 1	80%	70%	20%	10%
Communication & Coordination	Satisfied		% Yes	% Partially	% Not
	Objective 1	100%	100%	0%	0%
	Objective 2	100%	100%	0%	0%
	Objective 3	100%	100%	0%	0%
Work Environment	Satisfied		% Yes	% Partially	% Not
	Objective 1	100%	100%	0%	0%
	Objective 2	75%	50%	50%	0%

Figure 28. Evaluation tool. Level 2 statistical graphs

6.5 Level 3 Evaluation Summary Form

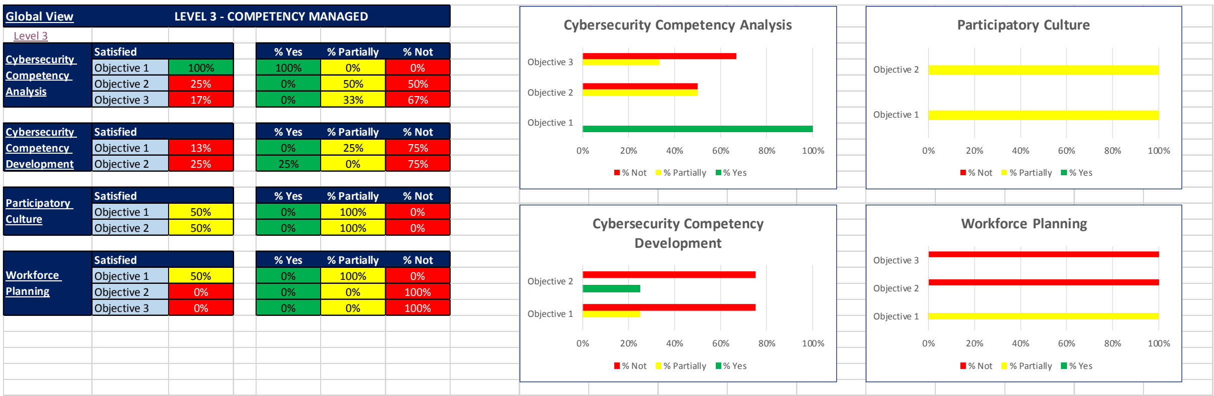
This form provides the summary of the Level 3 (Competency Managed) evaluation process. The user can have a global idea about the degree of deployment of the processes of the Competency Managed level. Figure 29 shows an example of the Competency Managed Level Summary Form.



Global View	LEVEL 3 - COMPETENCY MANAGED										
Level 3 Graphs											
Cybersecurity Competency Analysis	Objectives Satisfied		Practices								
	Total	47%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	
	Objective 1	100%	Yes	Yes	Yes						
	Objective 2	25%				Partial		No			
	Objective 3	17%					Partial		No	No	
Cybersecurity Competency Development	Objectives Satisfied		Practices								
	Total	19%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	
	Objective 1	13%	Partial	No	No	No					
	Objective 2	25%					No	No	No	Yes	
Participatory Culture	Objectives Satisfied		Practices								
	Total	50%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7		
	Objective 1	50%	Partial	Partial	Partial						
	Objective 2	50%				Partial	Partial	Partial	Partial		
Workforce Planning	Objectives Satisfied		Practices								
	Total	17%	Pract 1	Pract 2	Pract 3	Pract 4	Pract 5	Pract 6	Pract 7	Pract 8	Pract 9
	Objective 1	50%	Partial	Partial							
	Objective 2	0%			No	No					
	Objective 3	0%					No	No	No	No	No

Figure 29. Evaluation tool. Level 3, Competency Managed, evaluation summary form.

Figure 30 shows the statistical graphs representing the percentage of achievement for each process of level 3, Competency Managed.

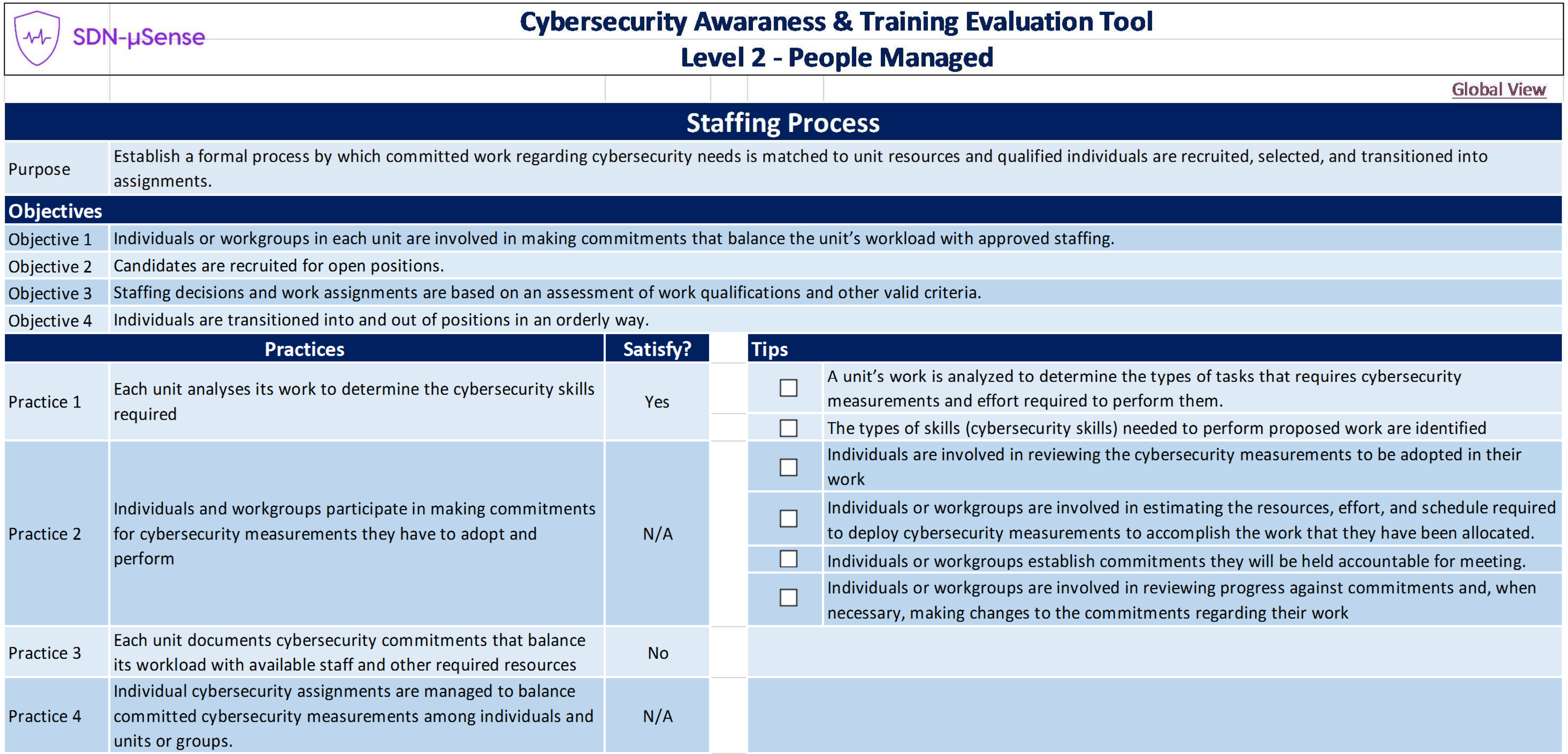


Global View	LEVEL 3 - COMPETENCY MANAGED				
Level 3					
Cybersecurity Competency Analysis	Satisfied		% Yes	% Partially	% Not
	Objective 1	100%	100%	0%	0%
	Objective 2	25%	0%	50%	50%
	Objective 3	17%	0%	33%	67%
Cybersecurity Competency Development	Satisfied		% Yes	% Partially	% Not
	Objective 1	13%	0%	25%	75%
	Objective 2	25%	25%	0%	75%
Participatory Culture	Satisfied		% Yes	% Partially	% Not
	Objective 1	50%	0%	100%	0%
	Objective 2	50%	0%	100%	0%
Workforce Planning	Satisfied		% Yes	% Partially	% Not
	Objective 1	50%	0%	100%	0%
	Objective 2	0%	0%	0%	100%
	Objective 3	0%	0%	0%	100%

Figure 30. Evaluation tool. Level 3 statistical graphs

6.6 Process Assessment Forms

Information about the level of deployment of each process in a company can be introduced in the Process data Entry Forms. Figure 31 and Figure 32 show the Process Assessment Forms of two processes: Staffing and Training and Development.



Cybersecurity Awareness & Training Evaluation Tool
Level 2 - People Managed

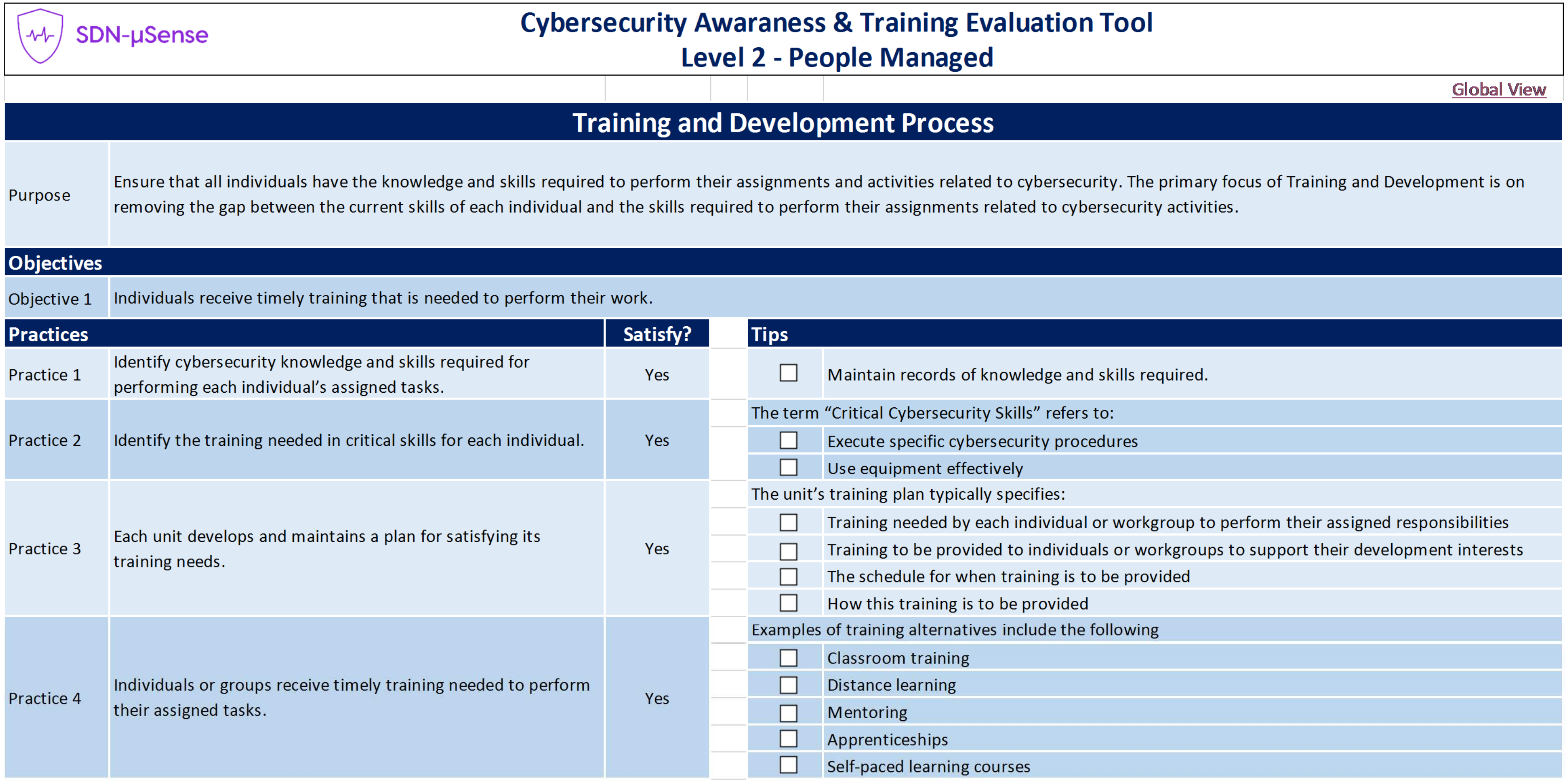
Global View

Staffing Process

Purpose	Establish a formal process by which committed work regarding cybersecurity needs is matched to unit resources and qualified individuals are recruited, selected, and transitioned into assignments.
Objectives	
Objective 1	Individuals or workgroups in each unit are involved in making commitments that balance the unit's workload with approved staffing.
Objective 2	Candidates are recruited for open positions.
Objective 3	Staffing decisions and work assignments are based on an assessment of work qualifications and other valid criteria.
Objective 4	Individuals are transitioned into and out of positions in an orderly way.

Practices		Satisfy?		Tips	
Practice 1	Each unit analyses its work to determine the cybersecurity skills required	Yes		□	A unit's work is analyzed to determine the types of tasks that requires cybersecurity measurements and effort required to perform them.
				□	The types of skills (cybersecurity skills) needed to perform proposed work are identified
Practice 2	Individuals and workgroups participate in making commitments for cybersecurity measurements they have to adopt and perform	N/A		□	Individuals are involved in reviewing the cybersecurity measurements to be adopted in their work
				□	Individuals or workgroups are involved in estimating the resources, effort, and schedule required to deploy cybersecurity measurements to accomplish the work that they have been allocated.
				□	Individuals or workgroups establish commitments they will be held accountable for meeting.
				□	Individuals or workgroups are involved in reviewing progress against commitments and, when necessary, making changes to the commitments regarding their work
Practice 3	Each unit documents cybersecurity commitments that balance its workload with available staff and other required resources	No			
Practice 4	Individual cybersecurity assignments are managed to balance committed cybersecurity measurements among individuals and units or groups.	N/A			

Figure 31. Evaluation tool. Staffing Process Assessment Form



SDN-μSense

Cybersecurity Awareness & Training Evaluation Tool
Level 2 - People Managed

Global View

Training and Development Process

Purpose	Ensure that all individuals have the knowledge and skills required to perform their assignments and activities related to cybersecurity. The primary focus of Training and Development is on removing the gap between the current skills of each individual and the skills required to perform their assignments related to cybersecurity activities.

Objectives

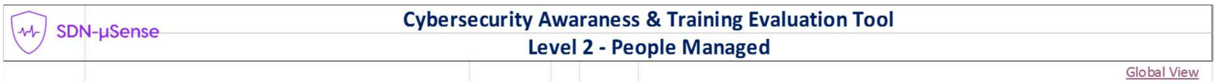
Objective 1	Individuals receive timely training that is needed to perform their work.

Practices		Satisfy?		Tips
Practice 1	Identify cybersecurity knowledge and skills required for performing each individual's assigned tasks.	Yes	□	Maintain records of knowledge and skills required.
Practice 2	Identify the training needed in critical skills for each individual.	Yes		The term "Critical Cybersecurity Skills" refers to:
			□	Execute specific cybersecurity procedures
			□	Use equipment effectively
Practice 3	Each unit develops and maintains a plan for satisfying its training needs.	Yes		The unit's training plan typically specifies:
			□	Training needed by each individual or workgroup to perform their assigned responsibilities
			□	Training to be provided to individuals or workgroups to support their development interests
			□	The schedule for when training is to be provided
			□	How this training is to be provided
Practice 4	Individuals or groups receive timely training needed to perform their assigned tasks.	Yes		Examples of training alternatives include the following
			□	Classroom training
			□	Distance learning
			□	Mentoring
			□	Apprenticeships
			□	Self-paced learning courses

Figure 32. Evaluation tool. Training & Development Process Assessment Form

The main components of the form are the followings:

1. **Header**: Shows the model level and process identification.



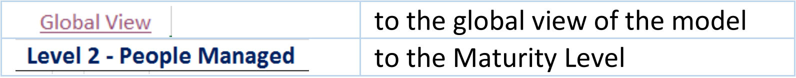
SDN-μSense

Cybersecurity Awaraness & Training Evaluation Tool

Level 2 - People Managed

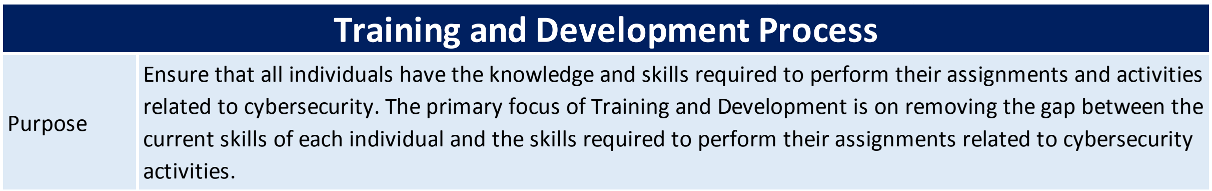
Global View

The header includes two links:



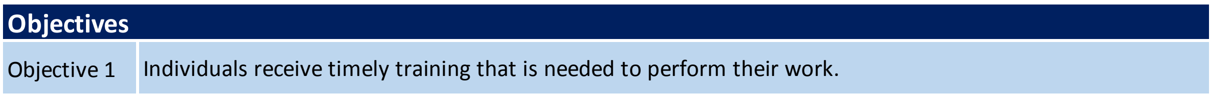
Global View	to the global view of the model
Level 2 - People Managed	to the Maturity Level

2. **Purpose of the Process**: a brief description of the purpose of the process.



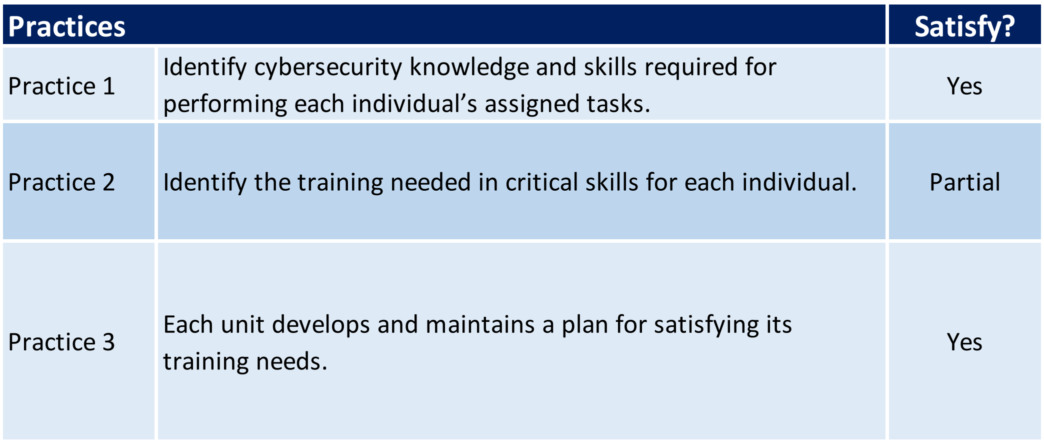
Training and Development Process	
Purpose	Ensure that all individuals have the knowledge and skills required to perform their assignments and activities related to cybersecurity. The primary focus of Training and Development is on removing the gap between the current skills of each individual and the skills required to perform their assignments related to cybersecurity activities.

3. **Objectives**: Objectives or goals to be achieved.



Objectives	
Objective 1	Individuals receive timely training that is needed to perform their work.

4. **Practices**: Practices to be deployed to achieve a specific goal of the process. On the right three columns to specify whether the practice has been deployed (“Yes”), not deployed (“No”) or partially deployed (“Partial”).



Practices		Satisfy?
Practice 1	Identify cybersecurity knowledge and skills required for performing each individual’s assigned tasks.	Yes
Practice 2	Identify the training needed in critical skills for each individual.	Partial
Practice 3	Each unit develops and maintains a plan for satisfying its training needs.	Yes

5. **Tips**: suggestions or examples that can be used to deploy the practice. Two types of tips are provided.

Practices	Tips	
Practice 1	□	Maintain records of knowledge and skills required.
Practice 2	The term “Critical Cybersecurity Skills” refers to:	
	□	Execute specific cybersecurity procedures
	□	Use equipment effectively
Practice 3	The unit’s training plan typically specifies:	
	□	Training needed by each individual or workgroup to perform their assigned responsibilities
	□	Training to be provided to individuals or workgroups to support their development interests
	□	The schedule for when training is to be provided
	□	How this training is to be provided

6.7 Assessment Process

The Evaluation Tool has been designed and developed to carry out an assessment of the deployment state of the maturity model in a company. This process could be done by the own company (self-assessment) or driven by external consultors (external appraisal).

The effort required to carry out the assessment process will depend on the company size. Table 29 provides an estimation of the required effort (in days) for the following company sizes:

- Micro SMES (less than 10 people).
- Small Companies (less than 100 people).
- Medium companies (less than 250 people).
- Single site large companies (more than 250 people)
- Multi-site large companies (more than 250 people).

Table 29. Effort estimation required to carry out the assessment

Size	Type of Appraisal	Effort
Micro SME	Self-assessment	5 days
Small (<100)	Two options:	
	1.Self-ssessment with the support of an external appraiser	7 days
	2.External appraisal (Documental Review + Interviews + Report Development + Final Results Presentation)	12 days

Size	Type of Appraisal	Effort
Medium (<=250)	External appraisal (Documental Review + Interviews + Report Development + Final Results Presentation)	12 days
Large Single-site	External appraisal (Documental Review + Interviews + Report Development + Final Results Presentation)	14 days
Large Multi-site	Depending on the number of sites. In the case of 2 sites, for example	24 days

The estimation has been done according to the following criteria:

Self-assessment Micro (5 days)

- 0.5 days approx. per process: 4 days
- 1 day of self-analysis of results

Self-assessment Small (7 days)

- 0.75 days approx. per process: 6 days
- 1 day of self-analysis of results

SME External Appraisal (12 days)

- 3 days of document review (3 hours approx. Per process: 24 hours)
- 1 day of interview per process + preparation of results report: 8 days
- 1 day presentation of results

Large Single site (14 days)

- 4 days of document review (4 hours approx. Per process: 32 hours)
- 1 day of interview per process: 8 days
- 1 day preparation of results report
- 1 day presentation of results

Large Multisite (in the case of two sites = 24 days)

- 5 days of document review (approx. 5 hours per process: 40 hours)
- 1 day of interview per process * 2 sites: 16 days
- 2 day preparation of results report
- 1 day presentation of results

7 Conclusions

It is very important for an energy related company to identify the training required in its personnel related to cybersecurity aspects, and not only identify these needs, also it is necessary to establish a mechanism to ensure that personnel have all the required information and training. This is a key aspect to avoid the risks that occur due to carelessness or unintentional errors of the employees. The model presented in this document supports companies in the energy sector to improve the way they train personnel in cybersecurity.

This document presents the Cybersecurity Awareness and Training Model for energy related personnel and processes. The proposed model has three main parts:

- The first part, the Cybersecurity maturity model has the objective of supporting energy related organisation in the definition of processes and practices that have to be defined and deployed in a company to improve the competency level of its personnel in cybersecurity aspects. It is based on People CMM. Although People CMM has five level of maturity, we have considered that the deployment of basic practices to acquire the required knowledge and skills in cybersecurity is achieved in the level 2 (People Managed) and in the level 3 (Competency Managed). The other levels of People CMM are aimed at organizations oriented to continuous improvement in an intensive way. These organizations must be able to quantitatively predict the benefit that a new improvement will bring them in their business activity. This extension of the model could be done afterwards due that the design of the model allows this kind of extensions.
- The second part, the Cybersecurity Competency model defines a set of knowledge and skill required to perform a specific job in a company. This competency model is based on the NIST NICE Framework but customising this framework to the specific cybersecurity necessities of the user roles defined in this project for an EPES stakeholder. A practical example of this competency model could be found in the Annex I, where for each user role is defined a table with information related to the assets, the threats associated to the assets, and the knowledge, skills and abilities.
- And finally, the evaluation tool supports the company to assess the processes that the energy related company has in place and to identify which are not implemented. Based on this information the tool provides information about the level of maturity of the company with respect to the implementation of the processes for training required in its personnel related to cybersecurity aspects.

8 References

[1] IEC, IEC 62443-2-1. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program., 2010.

[2] NERC, "CIP-004-6 — Cyber Security – Personnel & Training," 2014.

[3] ENISA, "Threat Landscape and Good Practice Guide for Smart Home and Converged Media.," 2014.

[4] NIST, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST Special Publication 800-181.," 2017.

[5] SEI, "People Capability Maturity Model (P-CMM) Version 2.0, Second Edition. Technical Report. Software Engineering Process Management," 2009.

[6] SDN-microSENSE, "D2.2. User & Stakeholder, Security and Privacy Requirements," Feb 2020.

[7] SDN-microSENSE, "D3.1. Risk Assessment Methodology of Energy Chain," May 2020.

[8] NIST, "NISTIR 7628 Revision 1. Guidelines for Smart Grid Cybersecurity. September 2014. National Institute of Standards and Technology. Department of Commerce. United State of America," Sep 2014.

[9] CEN-CENELEC-ETSI, "Smart Grid Coordination Group. Smart Grid Reference Architecture," Nov 2012.

[10] CEN, "European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors. CWA 16234:2014 Part 1," 2014.

[11] NIST, "National Initiative for Cybersecurity Education (NICE). Cybersecurity Workforce Framework," Aug 2017.

Annex I. Activity Roles in an Energy Company

This Annex contains a description of the different User Roles that have been defined for an Energy Company. Each Role description provides information about:

- The main activity of the role
- The list of company assets that are managed, controlled or operated by the roles.
- The list of threats suffered by the assets by the assets
- The list of knowledge, skills and abilities to be adopted by the role.

This information can be used by as a guideline to define the competences of each Role in the Company.

Executive Manager

Table 30 contains a detailed a description of the Executive Manager Role including assets, threats, knowledge, skills and abilities.

Table 30. Executive Manager Role Description.

Role	Executive Manager	
Role Description	The executive manager defines, executes, supervises and updates the operational plan of the organisation.	
Stakeholders	All	
Location	Office	
Assets		
Type	Category	Assets
Managed and controlled information	Inventory of Assets	Executive manager must have the control of all the information of the company.
	Operational	
	Historical information	
	Trending information:	
	Trading information	
Managed software	Databases:	Executive manager can access to different types of applications and databases can be accessed. Currently, there is a tendency to upload all the company's information to servers and repositories in the cloud.
	Applications	
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service, …
Used hardware	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, Mouse
Infrastructure	Facilities	Office, Control Centre.
Personnel	User	The executive manager is responsible of all the staff of the company.
	Operator	
	Administrator	
	Developer	
Threats & Vulnerabilities		

Type	Category
Unintentional damage (accidental)	Credential Steel. As in the case of the System Administrators, Security Administrator are especial target of the hackers in order to steal his/her credentials to enter into the system. Special attention should be taken about the information that is published in the social networks, and the mail received.
	Erroneous use or administration of devices and systems. Definition of weak security policies: generic user accounts and passwords, password that does not expire, …
	Using information from an unreliable source
	Unintentional change of data in an information system: LDAP, SIEM, SOC, …
	Inadequate design and planning or lack of adaptation. Wrong definition of security procedures
Damage/Loss (IT Assets)	Damages resulting from a penetration testing due to a wrong design.
	Damage caused by a third party that is collaborating with the security department.
	Loss of (integrity of) sensitive information, information device, storage media and documents.
	Destruction of records, devices or storage media, for example because of a ransomware attack.
	Information leakage.
Failures / Malfunction	Failure of devices or systems LDAP, SIEM, SOC, …
	Failure or disruption of service providers LDAP, SIEM, SOC, …
Eavesdropping / Interception / Hijacking	Interception of information
	Replay of messages
	Man in the Middle / Session hijacking
	Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.
Legal	Violation of laws or regulations / Breach of legislation
	Failure to meet contractual requirements
	Unauthorized use of copyrighted material

Knowledge

Category	Level	Knowledge
Communication Networks	Basic	• Basic knowledge about networks and communications • Knowledge of the basic structure, architecture, and design of modern communication networks • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
Cybersecurity	Basic	• Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization’s data assets
Laws and Regulations	Medium	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Basic	• Knowledge of organizational security policies
Organisational	Medium	• Knowledge of training and education policies, processes, and procedures

Organisational	Advanced	• Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information • Knowledge of deconfliction processes and procedures • Knowledge of organizational human resource policies, processes, and procedures. • Knowledge of organizational process improvement concepts and process maturity models • Knowledge about company organizational structure, roles and responsibilities • Targeting and Tasking
Technology Trend	Medium	• Knowledge of emerging technologies that have potential for exploitation

Skills

Category	Skill
Collection	• Skill to extract information from available tools and applications associated with collection requirements and collection operations management. • Skill to use collaborative tools and environments for collection operations.
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.
Information and Communication Technologies	• Skill in generating queries and reports.
Information Management	• Skill to access information on current assets available, usage. • Skill in using knowledge management technologies. • Skill in conducting social network analysis. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in preserving evidence integrity according to standard operating procedures or national standards. • Skill in complying with the legal restrictions for targeted information.
Organisational	• Skill in interfacing with customers. • Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results. • Skill in negotiating vendor agreements and evaluating vendor privacy practices. • Skill to analyze and assess internal and external partner reporting. • Skill in developing intelligence reports. • Skill in applying organization-specific systems analysis principles and techniques. • Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success.

Abilities

Category	Ability
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).

Information Management	- Ability to evaluate information for reliability, validity, and relevance. - Ability to ensure information security management processes are integrated with strategic and operational planning processes.
Laws and Regulations	- Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance. - Ability to author a privacy disclosure statement based on current laws.
Organisational	- Ability to interpret and translate customer requirements into operational action. - Ability to assess and forecast manpower requirements to meet organizational objectives. - Ability to determine the validity of workforce trend data. - Ability to utilize multiple intelligence sources across all intelligence disciplines. - Ability to apply approved planning development and staffing processes. - Ability to coordinate, collaborate and disseminate information to subordinate, lateral and higher-level organizations. - Ability to relate strategy, business, and technology in the context of organizational dynamics. - Ability to work across departments and business units to implement organization’s privacy principles and programs and align privacy objectives with security objectives. - Ability to work closely with authorizing officials and their designated representatives to help ensure that security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner - Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.

Security Administrator

Table 31 contains a detailed a description of the Security Administrator Role including assets, threats, knowledge, skills and abilities.

Table 31. Security Administrator Role Description.

Role	Security Administrator	
Role Description	Security Administrator is the person responsible for the overall security of the company, overseeing and enforcing the cybersecurity policy, identification of an organization's assets (including people, buildings, machines, systems and information assets), and the development, documentation, and implementation of policies and procedures for protecting these assets.	
Stakeholders	All	
Location	Typically, security administrator belongs to the system and informatics department which daily does the maintenance of the servers and dealing with cyber-security events. Control Centre in case of a cyberattack.	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Operational	System state in case of an attack.
	Historical information	Company staff, company assets, … Cybersecurity procedures, actions, evidences, …
	Trending information:	Historical suffered attacks.

	System Configuration	User credentials and access permission.
Managed software	Databases:	Active directory (LDAP) for authorization and authentication. Personnel records.
	Applications	Security Information Repository (SIEM, SOC, …)
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service, …
Used hardware	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, Mouse
Infrastructure	Facilities	Office, Control Centre.
Personnel	User	
	Operator	
	Administrator	
	Developer	

Threats & Vulnerabilities	
Type	**Category**
Unintentional damage (accidental)	Credential Steel. As in the case of the System Administrators, Security Administrator are especial target of the hackers in order to steal his/her credentials to enter into the system. Special attention should be taken about the information that is published in the social networks, and the mail received.
	Erroneous use or administration of devices and systems. Definition of weak security policies: generic user accounts and passwords, password that does not expire, …
	Using information from an unreliable source
	Unintentional change of data in an information system: LDAP, SIEM, SOC, …
	Inadequate design and planning or lack of adaptation. Wrong definition of security procedures
Damage/Loss (IT Assets)	Damages resulting from a penetration testing due to a wrong design.
	Damage caused by a third party that is collaborating with the security department.
	Loss of (integrity of) sensitive information, information device, storage media and documents.
	Destruction of records, devices or storage media, for example because of a ransomware attack.
	Information leakage.
Failures/ Malfunction	Failure of devices or systems LDAP, SIEM, SOC, …
	Failure or disruption of service providers LDAP, SIEM, SOC, …
Eavesdropping / Interception / Hijacking	Interception of information
	Replay of messages
	Man in the Middle / Session hijacking
	Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.
Legal	Violation of laws or regulations / Breach of legislation
	Failure to meet contractual requirements
	Unauthorized use of copyrighted material

Knowledge		
Category	**Level**	**Knowledge**

Collection	Medium	- Knowledge of collection disciplines and capabilities. - Knowledge of the available tools and applications associated with collection requirements and collection management.
Communication Networks Communication Networks	Medium	- Advanced knowledge about a communication technology - Knowledge of the basic structure, architecture, and design of modern communication networks - Knowledge on network management
	Advanced	- Basic knowledge about networks and communications - Knowledge about industrial and TCP/IP protocols - Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
Cybersecurity	Medium	- Knowledge of cryptography and cryptographic key management concepts: encryption algorithms and methodologies
	Advanced	- Knowledge of authentication, authorization, and access control methods - Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities - Knowledge of cyber defense and information security policies, procedures, and regulations - Knowledge of ethical hacking principles and techniques - Knowledge of concepts and practices of processing digital forensic data - Knowledge of incident categories and incident responses - Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization - Knowledge of risk management processes - Knowledge of cybersecurity and privacy principles - Knowledge of cyber threats and vulnerabilities
Information and Communication Technologies	Basic	- Knowledge of computer programming principles - Knowledge of software design tools, methods, and techniques
	Medium	- Knowledge of database management systems, query languages, table relationships, and views - Knowledge about the design and development of hardware devices - Knowledge of information technology (IT) architectural concepts and frameworks - Knowledge of the characteristics of physical and virtual data storage media - Knowledge of operating systems - Knowledge of systems engineering theories, concepts, and methods - Knowledge of how Internet applications work
	Advanced	- Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly
Information Management	Basic	- Knowledge of the capabilities and functionality associated with content creation and processing technologies
	Medium	- Knowledge of data administration and data standardization policies
	Advanced	- Knowledge of sources, characteristics, and uses of the organization's data assets - Knowledge of critical information technology

Laws and Regulations	Medium	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Medium	• Knowledge of organizational process improvement concepts and process maturity models • Knowledge about company organizational structure, roles and responsibilities
	Advanced	• Knowledge of organizational security policies
Technology Trend	Basic	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of emerging technologies that have potential for exploitation

Skills

Category	Skill
Cybersecurity	• Skill in developing and applying security system access controls. • Skill in maintaining directory services. (e.g., Microsoft Active Directory, LDAP, etc.). • Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.). • Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. • Skill in discerning the protection needs (i.e., security controls) of information systems and networks. • Skill in evaluating the adequacy of security designs. • Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege, etc.). • Skill in assessing security systems designs. • Skill in translating operational requirements into protection needs (i.e., security controls). • Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • Skill to use cyber defense Service Provider reporting structure and processes within one's own organization. • Skill in the use of penetration testing tools and techniques. • Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics). • Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. • Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK). • Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems). • Skill in deep analysis of captured malicious code (e.g., malware forensics). • Skill in reviewing logs to identify evidence of past intrusions. • Skill in using incident handling methodologies. • Skill in processing digital evidence, to include protecting and making legally sound copies of evidence. • Skill in assessing and/or estimating effects generated during and after cyber operations. • Skill to design incident response for cloud service models.

	• Skill to respond and take local actions in response to threat sharing alerts from service providers. • Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). • Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles. • Skill in designing security controls based on cybersecurity principles and tenets. • Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.). • Skill in identifying critical target elements, to include critical target elements for the cyber domain. • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. • Skill in recognizing and categorizing types of vulnerabilities and associated attacks. • Skill in conducting application vulnerability assessments. • Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning). • Skill in identifying cyber threats which may jeopardize organization and/or partner interests. • Skill in interpreting vulnerability scanner results to identify vulnerabilities. • Skill to anticipate new security threats. • Skill to develop insights about the context of an organization's threat environment • Skill to identify cybersecurity and privacy issues that stem from connections with internal and external customers and partner organizations.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill to access the databases where plans/directives/guidance are maintained. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization's data assets. • Skill in using knowledge management technologies. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in conducting social network analysis. • Skill in evaluating information for reliability, validity, and relevance. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in complying with the legal restrictions for targeted information.
Organisational	• Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success.
Personal Skills	• Skill in talking to others to convey information effectively. • Skill in preparing and presenting briefings. • Skill in preparing plans and related correspondence. • Skill in reviewing and editing plans. • Skill in writing effectiveness reports. • Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.
Abilities	
Category	**Ability**

Cybersecurity	• Ability to prioritize and allocate cybersecurity resources correctly and efficiently. • Ability to establish and maintain automated security control assessments • Ability to conduct a comprehensive assessment of the management, operational, and technical security controls. • Ability to assesses a security plan to help ensure that the plan provides a set of security controls for the system that meet the stated security requirements. • Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations. • Ability to recognize the unique aspects of the Communications Security (COMSEC) environment and hierarchy. • Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities. • Ability to prepare the final security assessment report containing the results and findings from the assessment. • Ability to apply secure system design tools, methods and techniques. • Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • Ability to conduct systems security engineering activities (NIST SP 800-16).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	• Ability to analyze test data. • Ability to evaluate information for reliability, validity, and relevance. • Ability to ensure information security management processes are integrated with strategic and operational planning processes.
Laws and Regulations	• Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives. • Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance. • Ability to author a privacy disclosure statement based on current laws.
Organisational	• Ability to ensure the organization has adequately trained personnel to assist in complying with security requirements in legislation, Executive Orders, policies, directives, instructions, standards, and guidelines. • Ability to coordinate with senior leadership of an organization to provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization. • Ability to coordinate with senior leadership of an organization to develop a risk management strategy for the organization providing a strategic view of security-related risks for the organization. • Ability to coordinate with senior leadership of an organization to facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization. • Ability to coordinate with senior leadership of an organization to provide oversight for all risk management-related activities across the organization to help ensure consistent and effective risk acceptance decisions.

	• Ability to coordinate with senior leadership of an organization to ensure that authorization decisions consider all factors necessary for mission and business success. • Ability to coordinate with senior leadership of an organization to identify the organizational risk posture based on the aggregated risk from the operation and use of the systems for which the organization is responsible. • Ability to work closely with authorizing officials and their designated representatives to help ensure that an organization-wide security program is effectively implemented resulting in adequate security for all organizational systems and environments of operation. • Ability to work closely with authorizing officials and their designated representatives to help ensure that security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles. Ability to work closely with authorizing officials and their designated representatives to help ensure that security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner. • Ability to approve security plans, memorandums of agreement or understanding, plans of action and milestones, and determine whether significant changes in the systems or environments of operation require reauthorization. • Ability to serve as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and system security officers on the allocation of security controls as system-specific, hybrid, or common controls. • Ability to ensure information system security, acquisition personnel, legal counsel, and other appropriate advisors and stakeholders are participating in decision making from system concept definition/review and are involved in, or approve of, each milestone decision through the entire system life cycle for systems.

Power Plant Operator

Table 32 contains a detailed a description of the Power Plant Operator Role including assets, threats, knowledge, skills and abilities.

Table 32. Power Plant Operator Role Description.

Role	Power Plant Operator
Role	**Power Plant Operator**
Role Description	Power plant operators monitor, control, and configure the power plant operation. They use control boards (SCADA[22]) to distribute power from generators among loads and regulate the output of several generators. The main task of the plant operator is the same: • Ensuring the energy production according to the energy market agreements. • Surveillance the correct operation of the plant and the electrical substation uprating the electrical power to the distribution or transmission level. • Detect functional failures in the generation process.

[22] SCADA. Supervisory Control And Data Acquisition.

	• He can act over trackers and inverters (PV plants) • Maintain the electronic equipment in perfect work status	
Stakeholders	Energy Producers.	
Location	In large power plants, the physical process is monitored and controlled from the control room of the plant, where the SCADA is located. In the case of the smaller renewable plants the supervision is done remotely, in the central headquarters of the Energy providers.	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of assets.	Power plant components and devices.
	Operational	Status, alarms, events, shortage, disturbances, ...
	Historical information	Production data, weather and irradiation data, alarm summaries, general events, maintenance dates and registers
	Trending information:	Production data, weather data, irradiation data
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files, …
Managed software	Databases:	Data Repositories: configuration files, asset inventory, fault registry, … Backup repositories. In case of an attack the plant operator should be able to restore the whole system form the backup.
	Applications	SCADA. It receives information from the process and visualises the state of the components state and main process measurements. It also allows the operation, sending commands to the actuators.
		Forecasting Tools. In the renewable generation plant the forecasting tools provides information about the weather condition that affect the energy production.
		Automatic Voltage Regulator and Governor Control. The AVR is the system for adjusting the power output of multiple generators at different power plants, in response to changes in the load.
		Automatic generation control (AGC) is a system for adjusting the power output of multiple generators at different power plants
		Fault Management.
		PLC software and program versions
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service, …
Used hardware	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, Mouse
Infrastructure	Facilities	Power Plant, Control Centre (in case of remote supervision of the plant).
Threats & Vulnerabilities		
Type	**Category**	

Unintentional damage (accidental)	Credential Steel. Erroneous use or administration of devices and systems: weak password management, Using information from an unreliable source Unintentional change of data in an information system. Inadequate design and planning or lack of adaptation.
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information: energy consumption, session data, access control data, ...
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and Information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge

Category	Level	Knowledge
Collection	Basic	• Knowledge of collection management processes, capabilities, and limitations. • Knowledge of collection disciplines and capabilities.
Communication Networks	Basic	• Basic knowledge about networks and communications • Knowledge of the basic structure, architecture, and design of modern communication networks • Knowledge about industrial and TCP/IP protocols • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods. • Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. • Knowledge of cyber defense and information security policies, procedures, and regulations. • Knowledge of ethical hacking principles and techniques. • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization • Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
	Advanced	• Knowledge of incident categories and incident responses
Information and Communication Technologies	Basic	• Knowledge of database management systems, query languages, table relationships, and views • Knowledge about the design and development of hardware devices

		• Knowledge of information technology (IT) architectural concepts and frameworks • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of the characteristics of physical and virtual data storage media • Knowledge of operating systems • Knowledge of systems engineering theories, concepts, and methods
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization's data assets • Knowledge of data administration and data standardization policies • Knowledge of the capabilities and functionality associated with content creation and processing technologies • Knowledge of critical information technology
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Advanced	• Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information. • Knowledge of intelligence disciplines • Knowledge of training and education policies, processes, and procedures • Knowledge of organizational process improvement concepts and process maturity models • Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies • Knowledge of organizational security policies
Technology Trend	Basic	• Knowledge of emerging technologies that have potential for exploitation

Skills	
Category	**Skill**
Cybersecurity	• Skill in applying confidentiality, integrity, and availability principles. • Skill in identifying critical target elements, to include critical target elements for the cyber domain.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill to access the databases where plans/directives/guidance are maintained. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization's data assets. • Skill in using knowledge management technologies. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in complying with the legal restrictions for targeted information.
Organisational	• Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success.

Abilities	
Category	**Ability**
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	• Ability to evaluate information for reliability, validity, and relevance.
Organisational	• Ability to effectively collaborate via virtual teams. • Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.

Facility Operator

Table 33 contains a detailed a description of the Facility Operator Role including assets, threats, knowledge, skills and abilities.

Table 33. Facility Operator

Role	Facility Operator	
Role	**Facility Operator**	
Role Description	Engineer that operates the electrical equipment of the power plant: RTUs, inverters, …	
Stakeholders	Energy producers.	
Location	Power Plants	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of assets.	Power plant components and devices.
	Operational	Status, alarms, events, shortage, disturbances, ...
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files, …
Managed software	Databases:	Data Repositories: configuration files, asset inventory, fault registry, … Backup repositories. In case of an attack the plant operator should be able to restore a device.
	Applications	Configuration tools
	Firmware	RTU, IED
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service, …
Used hardware	Smart grid	RTU, IED, PLC, DCS, …
	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...
	Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point, …
	Media devices	External storage
Infrastructure	Facilities	Power Plant.

Threats & Vulnerabilities

Type	Category
Unintentional damage (accidental)	Credential Steel. Erroneous use or administration of devices and systems: weak password management, … Using information from an unreliable source, for example a non-authenticated firmware, Unintentional change of data in an information system, wrong configuration of devices.
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information: configuration files, access control data, ...
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and Information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge

Category	Level	Knowledge
Communication Networks	Medium	• Basic knowledge about networks and communications • Knowledge of the basic structure, architecture, and design of modern communication networks • Knowledge on network management • Knowledge about industrial and TCP/IP protocolos
Cybersecurity	Basic	• Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
Information and Communication Technologies	Medium	• Knowledge about the design and development of hardware devices • Knowledge of information technology (IT) architectural concepts and frameworks • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of operating systems • Knowledge of systems engineering theories, concepts, and methods
Information Management	Medium	• Knowledge of sources, characteristics, and uses of the organization’s data assets

Skills

Category	Skill
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).

Information Management	• Skill to access information on current assets available, usage. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Abilities	
Category	**Ability**
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Organisational	• Ability to effectively collaborate via virtual teams.

Field Engineer

Table 34 contains a detailed a description of the Field Engineer Role including assets, threats, knowledge, skills and abilities.

Table 34. Field Engineer Role Description.

Role	**Field Engineer**	
Role	**Field Engineer**	
Role Description	Engineer that is always present in the facility and may be instructed by the System Administrator or the facility operator to perform specific action for maintenance or infrastructure protection.	
Stakeholders	Energy producers.	
Location	Power Plants	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of assets.	Power plant components and devices.
	Operational	Status, alarms, events, shortage, disturbances, ... of the power plant equipment.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files, …
Managed software	Databases:	Data Repositories: configuration files, asset inventory, fault registry, … Backup repositories. In case of an attack the plant operator should be able to restore a device.
	Applications	Configuration tools
	Firmware	RTU
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service, …
Used hardware	Smart grid	RTU, Inverter, …
	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...

	Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point, …
	Media devices	External storage
Infrastructure	Facilities	Power Plant.

Threats & Vulnerabilities

Type	Category
Unintentional damage (accidental)	Credential Steel. Erroneous use or administration of devices and systems (e.g., weak password management). Using information from an unreliable source, install wrong firmware, Unintentional change of data in an information system, wrong configuration of devices.
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., configuration files, access control data).
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and Information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge

Category	Level	Knowledge
Communication Networks	Basic	• Basic knowledge about networks and communications. • Advanced knowledge about a communication technology. • Knowledge on network management. • Knowledge about industrial and TCP/IP protocols • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
Communication Networks	Medium	• Knowledge of the basic structure, architecture, and design of modern communication networks
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods • Knowledge of cyber defense and information security policies, procedures, and regulations. • Knowledge of ethical hacking principles and techniques. • Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
	Medium	• Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities. • Knowledge of incident categories and incident responses
	Basic	• Knowledge about the design and development of hardware devices

Information and Communication Technologies	Medium	• Knowledge of the characteristics of physical and virtual data storage media
Information Management	Advanced	• Knowledge of sources, characteristics, and uses of the organization’s data assets
Technology Trend	Basic	• Knowledge of emerging technologies that have potential for exploitation

Skills

Category	Skill
Cybersecurity	• Skill in assessing security systems designs. • Skill in translating operational requirements into protection needs (i.e., security controls). • Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles. • Skill in identifying critical target elements, to include critical target elements for the cyber domain.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyse that data). • Skill in developing data dictionaries. • Skill in developing data models. • Skill in recognizing relevance of information. • Skill in conducting information searches.

Abilities

Category	Ability
Cybersecurity	• Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations. • Ability to recognize the unique aspects of the Communications Security (COMSEC) environment and hierarchy. • Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities. • Ability to prepare the final security assessment report containing the results and findings from the assessment. • Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	• Ability to evaluate information for reliability, validity, and relevance.
Personal Abilities	• Ability to effectively collaborate via virtual teams.

	• Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.

System Operator/Engineer

Table 35 contains a detailed a description of the System Operator and Engineer Role including assets, threats, knowledge, skills and abilities.

Table 35. System Operator / Engineer Role Description.

Role	System Operator / Engineer	
Role	**System Operator / Engineer**	
Role Description	The system operator is a person who controls and supervises the electric grid or a big part of it and is responsible for coordinating its various aspects to ensure grid's availability and health. It is the entity responsible for the reliability of its local transmission and/or distribution system, and that operates or directs the operations of the grid facilities.	
Stakeholders	TSO & DSO	
Location	Control Centre.	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators.
	Operational	Status, alarms, events, shortage, disturbances
	Historical information	Production data, weather data, alarm summaries, general events, maintenance dates and registers
	Trending information:	Consumption habits that can predict the near future consumption and renewable generation.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Data Repositories, Backups,
	Applications	SCADA. It receives information from the electrical substations and visualises the state of the substation components (mainly circuit breakers or disconnection switches) and the electrical measurements. It also allows the operation, sending commands.
		Forecasting Tools,
		State Estimation,
		Load Shedding. They are useful in preventing system collapse in cases where the system generation is insufficient to match up to the load.
		Fault Management,
		Automatic Generation Control (AGC). AGC loop is a secondary frequency control loop that is concerned with fine-tuning the system frequency to its nominal value. The function of the AGC loop is to make corrections to inter-area tie-line flow and frequency deviation

		Volt/VAR Control. DSO is responsible to maintain the distribution network voltage level.
		Advanced Metering Infrastructure (AMI). It manages consumer data through the smart meters allowing the DSO to increase reliability, incorporate renewable energy, and provide consumers with efficient billing process, granular consumption monitoring through Demand Side Management.
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service.
Used hardware	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, Mouse
Infrastructure	Facilities	Office, Control Centre.

Threats & Vulnerabilities	
Type	**Category**
Unintentional damage (accidental)	Credential Steel. Erroneous use or administration of devices and systems: weak password management, Using information from an unreliable source Unintentional change of data in an information system. Inadequate design and planning or lack of adaptation.
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information: energy consumption, session data, access control data, ...
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and Information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge		
Category	**Level**	**Knowledge**
Collection	Basic	• Knowledge of the available tools and applications associated with collection requirements and collection management.
Communication Networks	Basic	• Basic knowledge about networks and communications • Knowledge about industrial and TCP/IP protocols
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods. • Knowledge of cyber defense and information security policies, procedures, and regulations. • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities

	Advanced	• Knowledge of incident categories and incident responses
Information and Communication Technologies	Basic	• Knowledge of database management systems, query languages, table relationships, and views. • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly. • Knowledge of systems engineering theories, concepts, and methods.
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization's data assets • Knowledge of data administration and data standardization policies
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Basic	• Knowledge of deconfliction processes and procedures • Knowledge of organizational human resource policies, processes, and procedures. • Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies
Technology Trend	Basic	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics. • Knowledge of emerging technologies that have potential for exploitation

Skills

Category	Skill
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles. • Skill in identifying critical target elements, to include critical target elements for the cyber domain.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill to access the databases where plans/directives/guidance are maintained. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization's data assets. • Skill in using knowledge management technologies. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in complying with the legal restrictions for targeted information.
Organisational	• Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success.

Abilities

Category	Ability
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	• Ability to evaluate information for reliability, validity, and relevance.
Personal Abilities	• Ability to effectively collaborate via virtual teams. • Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.

Energy Trader

Table 36 contains a detailed a description of the Energy Trader Role including assets, threats, knowledge, skills and abilities.

Table 36. Energy Trader Role Description.

Role	Energy Trader	
Role	**Energy Trader**	
Role Description	Energy trader is responsible for the trading of Energy between cooperating parties. Coordinates with the Systems Operator to achieve the desired status of the grid.	
Stakeholders	TSO	
Location	Control Centre	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Historical information that must be storage by low.	Energy Trader should have the necessary market knowledge, potential customers and some knowledge of the legal framework. Energy market transactions: generation and consumption offer, prices matching, bilateral contracts.
	Trending information	Historical information about generation and consumption Historical information about energy market transactions Marker evolution
	Trading information	Energy market agents Historical information about generation and consumption Historical information about energy market transactions Marker evolution
	System Configuration	Grid topology: transmission grid, generation centres, big consumers, primary substations, ... Energy actors (e.g., generators, aggregators, DSOs, energy traders). Information about the system operators,
Managed software	Databases:	Market Agents, Generation and Consumption Bids, Bilateral contracts, Billing.
	Applications	Market Operator Information System
Used services	Oriented to the staff	Mail Service, Authentication Service, Office applications Energy market information services (e.g., offers, contract, evolution, adjustment).
	Oriented to the network	File service, network service, name service, address service.
Used hardware	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...

	Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point.
	Media devices	External storage
	Displays	Monitor, Beamer for internal meetings
	Human interaction	Dock Station
Infrastructure	Facilities	Access to the Company Premises

Threats & Vulnerabilities	
Type	**Category**
Unintentional damage (accidental)	Credential Steel. Erroneous use or administration of energy market application (e.g., weak password management). Using information from an unreliable source. Unintentional change of data in an information system.
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., energy transaction, bank accounts).
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge		
Category	**Level**	**Knowledge**
Collection	Basic	• Knowledge of collection disciplines and capabilities.
Communication Networks	Basic	• Basic knowledge about networks and communications • Knowledge about industrial and TCP/IP protocols • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods • Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities • Knowledge of cyber defense and information security policies, procedures, and regulations. • Knowledge of incident categories and incident responses • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization • Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles

		• Knowledge of cyber threats and vulnerabilities
Information and Communication Technologies	Basic	• Knowledge of database management systems, query languages, table relationships, and views. • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of the characteristics of physical and virtual data storage media • Knowledge of operating systems. • Knowledge of how Internet applications work
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization’s data assets • Knowledge of data administration and data standardization policies • Knowledge of the capabilities and functionality associated with content creation and processing technologies
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
Organisational	Basic	• Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies

Skills	
Category	**Skill**
Collection	• Extract information from available tools and applications associated with collection requirements and collection operations management. • Skill to use collaborative tools and environments for collection operations.
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in identifying critical target elements.
Information and Communication Technologies	• Skill in generating queries and reports and using Boolean operators to construct simple and complex queries. • Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.).
Information Management	• Skill to access information on current assets available, usage. • Skill in using knowledge management technologies. • Skill in conducting social network analysis. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in preserving evidence integrity according to standard operating procedures or national standards. • Skill in complying with the legal restrictions.
Organisational	• Skill in interfacing with customers. • Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results. • Skill in negotiating vendor agreements and evaluating vendor privacy practices. • Skill to analyse and assess internal and external partner reporting. • Skill in developing intelligence reports. • Skill in applying organization-specific systems analysis principles and techniques. • Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success. • Skill to express orally and in writing the relationship between intelligence capability limitations and decision-making risk and impacts on the overall operation.

	• Skill in talking to others to convey information effectively. • Skill in preparing and presenting briefings. • Skill in reviewing and editing plans. • Skill in writing effectiveness reports. • Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.
Technology Trend	• Skill to remain aware of evolving technical infrastructures.
Abilities	
Category	**Ability**
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). Ability to evaluate information for reliability, validity, and relevance.
Information Management	• Ability to evaluate information for reliability, validity, and relevance.
Laws and Regulations	• Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance. • Ability to author a privacy disclosure statement based on current laws.
Organisational	• Ability to answer questions in a clear and concise manner. • Ability to prepare and present briefings. • Ability to communicate effectively • Ability to produce technical documentation. • Ability to apply collaborative skills and strategies. • Ability to effectively collaborate via virtual teams. • Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.

AMI and Demand Side Manager

Table 37 contains a detailed a description of the AMI and Demand Side Manager Role including assets, threats, knowledge, skills and abilities.

Table 37. AMI and Demand Side Manager Role Description.

Role	**AMI & Demand Side Manager**	
Role	**AMI and Demand Side Manager**	
Role Description	Gathering real-time meter readings and managing load control switching mechanisms	
Stakeholders	DSO	
Location	Control Centre	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Smart meters, concentrators, smart appliances.
	Operational	Status, alarms, events, shortage, disturbances

	Historical information	Consumption / generation data, demand respond actions, flexibility requests.
	Trending information:	Consumption habits that can predict the near future consumption and renewable generation.
	Trading information	End user data for billing.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Meter data management system. It stores consumption/generation data gathered from the metering infrastructure.
	Applications	Demand Side Management.
Used services	Oriented to the staff	Mail, print service, authentication service.
	Oriented to the network	File service, network service, name service, address service.
Used hardware	Smart Meters	End devices, local and neighbourhood network access point, External displays, home automation components, AMI head end.
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Media devices	External storage.
Infrastructure	Facilities	Office.
Threats & Vulnerabilities		
Type	**Category**	
Unintentional damage (accidental)	Credential Steel. Erroneous use or administration of energy market application (e.g., weak password management). Using information from an unreliable source. Unintentional change of data in an information system.	
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., energy consumed or generated, bank accounts).	
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.	
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions	
Nefarious Activity / Abuse	All threats should be considered.	
Knowledge		
Category	**Level**	**Knowledge**
Communication Networks	Basic	• Knowledge of collection disciplines and capabilities. • Knowledge of the available tools and applications associated with collection requirements and collection management.
	Medium	• Knowledge of collection management processes, capabilities, and limitations.

Cybersecurity	Basic	• Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities • Knowledge of cybersecurity and privacy principles
	Medium	• Knowledge of incident categories and incident responses
	Advanced	• Knowledge of authentication, authorization, and access control methods
Communication Networks	Basic	• Knowledge about industrial and TCP/IP protocols
	Medium	• Knowledge about networks and communications
Information and Communication Technologies	Basic	• Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly. • Knowledge of operating systems
	Medium	• Knowledge of database management systems, query languages, table relationships, and views • Knowledge about the design and development of hardware devices
Information Management	Basic	• Knowledge of the capabilities and functionality associated with content creation and processing technologies • Knowledge of critical information technology
	Medium	• Knowledge of sources, characteristics, and uses of the organization's data assets • Knowledge of data administration and data standardization policies
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Basic	• Knowledge of deconfliction processes and procedures. • Knowledge of organizational process improvement concepts and process maturity models
Technology Trend	Basic	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics. • Knowledge of emerging technologies that have potential for exploitation

Skills	
Category	**Skill**
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill to access the databases where plans/directives/guidance are maintained. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization's data assets. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in complying with the legal restrictions for targeted information.
Organisational	• Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success. • Skill in talking to others to convey information effectively.

Abilities	
Category	**Ability**
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	• Ability to evaluate information for reliability, validity, and relevance.
Personal Abilities	• Ability to effectively collaborate via virtual teams. • Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.

Operational Technology Manager / Communication Administrator

Table 38 contains a detailed a description of the Operational Technology and Communication Administrator Role including assets, threats, knowledge, skills and abilities.

Table 38. Operational Manager / Communication Administrator Role Description.

Role	Operational Technology Manager Communication Administrator
Role	**Operational Technology Manager / Communication Administrator**
Role Description	The person responsible of the OT security and functioning at the control Room and in the Substations. Communication Admin is responsible for the availability of the communication network. She is the one that is responsible for allowing or cutting off traffic in the communication network, identifying cyberattacks etc. Works closely with the Security Admin. IT Systems and Network Administrator: This person manages and oversees the operation of the entire IT equipment.
Stakeholders	All
Location	Premises, buildings and offices, control centre, data centre.

Assets		
Type	**Category**	**Assets**
Managed and controlled information	Operational	Status, alarms, events, shortage, disturbances, of the communication network.
	Trending information:	Network data, band width consumption, past problems.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Equipment Inventory: communication devices, IT servers, desktop, laptops, smart mobiles. Backup repository. Collects data and answer to requests. Server logs.
	Applications	Asset Management System.

		The Communication Admin should check the logs regarding any login attempts. She should also check the appropriate monitoring system for any anomalies on the communication network.
	Operating Systems	
	Device Drivers	
	Firmware	
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service.
	Cloud services	SaaS, IaaS
Used hardware	Servers	Hardware servers
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point.
	Media devices	External storage
Infrastructure	Facilities	Office, control centre, substations, power plants.

Threats & Vulnerabilities

Type	Category
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel). Erroneous use or administration of energy market application (e.g., weak password management). Using information from an unreliable source. Unintentional change of data in an information system. Inadequate design or lack of adaptation
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., energy consumed or generated, bank accounts).
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge

Category	Level	Knowledge
Collection	Basic	• Knowledge of collection management processes, capabilities, and limitations. • Knowledge of collection disciplines and capabilities. • Knowledge of the available tools and applications associated with collection requirements and collection management.
Communication Networks	Medium	• Advanced knowledge about a communication technology. • Knowledge on network management • Knowledge about industrial and TCP/IP protocols

		• Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
	Advanced	• Basic knowledge about networks and communications • Knowledge of the basic structure, architecture, and design of modern communication networks
Cybersecurity	Basic	• Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities • Knowledge of cyber defense and information security policies, procedures, and regulations • Knowledge of cryptography and cryptographic key management concepts: encryption algorithms and methodologies • Knowledge of ethical hacking principles and techniques • Knowledge of concepts and practices of processing digital forensic data • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization • Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
	Medium	• Knowledge of authentication, authorization, and access control methods
	Advanced	• Knowledge of incident categories and incident responses
Information and Communication Technologies	Basic	• Knowledge of database management systems, query languages, table relationships, and views • Knowledge about the design and development of hardware devices • Knowledge of information technology (IT) architectural concepts and frameworks • Knowledge of operating systems • Knowledge of computer programming principles • Knowledge of software design tools, methods, and techniques • Knowledge of how Internet applications work
	Medium	• Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of systems engineering theories, concepts, and methods
	Advanced	• Knowledge of the characteristics of physical and virtual data storage media
Information Management	Basic	• Knowledge of the capabilities and functionality associated with content creation and processing technologies • Knowledge of critical information technology
	Medium	• Knowledge of data administration and data standardization policies
	Advanced	• Knowledge of sources, characteristics, and uses of the organization's data assets
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Basic	• Knowledge of organizational human resource policies, processes, and procedures. • Knowledge of training and education policies, processes, and procedures

		• Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies • Knowledge of organizational security policies
Organisational	Advanced	• Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information • Knowledge of organizational process improvement concepts and process maturity models
Technology Trend	Basic	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of machine learning theory and principles • Knowledge of emerging technologies that have potential for exploitation

Skills	
Category	**Skill**
Communication Networks	• Skill in survey, collection, and analysis of wireless LAN metadata. • Skill in using non-attributable networks. • Skill in using various open source data collection tools (e.g., online trade, DNS, mail). • Skill in establishing a routing schema. • Skill in applying various subnet techniques (e.g., CIDR) • Skill in setting up physical or logical sub-networks that separate an internal local area network (LAN) from other untrusted networks. • Skill in analysing a target's communication networks. • Skill in analysing essential network data (e.g., router configuration files, routing protocols). • Skill in analysing traffic to identify network devices. • Skill in determining the physical location of network devices. • Skill in identifying a target’s communications networks. • Skill in identifying a target's network characteristics. • Skill in identifying the devices that work at each level of protocol models. • Skill in interpreting traceroute results, as they apply to network analysis and reconstruction. • Skill in using research methods including multiple, different sources to reconstruct a target network. • Skill in analysing network traffic capacity and performance characteristics. • Skill in diagnosing connectivity problems. • Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches. • Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). • Skill in using network management tools to analyse network traffic patterns (e.g., simple network management protocol). • Skill in using protocol analysers. • Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. • Skill in implementing and testing network infrastructure contingency and recovery plans.

	• Skill in performing packet-level analysis. • Skill in analysing target communications internals and externals collected from wireless LANs. • Skill in extracting information from packet captures. • Skill in navigating network visualization software.
Cybersecurity	• Skill in applying host/network access controls (e.g., access control list). • Skill in developing and applying security system access controls. • Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating). • Skill in recognizing and interpreting malicious network activity in traffic. • Skill in recognizing denial and deception techniques of the target. • Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. • Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. • Skill in implementing, maintaining, and improving established network security practices. • Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). • Skill in securing network communications. • Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). • Skill in integrating black box security testing tools into quality assurance process of software releases. • Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems). • Skill in applying security controls. • Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege). • Skill in assessing security systems designs. • Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). • Skill in auditing firewalls, perimeters, routers, and intrusion detection systems. • Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments. • Skill in developing and deploying signatures. • Skill in using Virtual Private Network (VPN) devices and encryption. • Skill in reading and interpreting signatures (e.g., snort). • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). • Skill in the use of penetration testing tools and techniques. • Skill in collecting data from a variety of cyber defense resources. • Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics). • Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. • Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort). • Skill in analysing malware. • Skill in performing impact/risk assessments.

	• Skill in applying confidentiality, integrity, and availability principles. • Skill in designing security controls based on cybersecurity principles and tenets. • Skill in identifying critical target elements, to include critical target elements for the cyber domain. • Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. • Skill in recognizing and categorizing types of vulnerabilities and associated attacks. • Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap). • Skill in interpreting vulnerability scanner results to identify vulnerabilities.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in maintaining databases. (e.g., backup, restore, delete data, transaction log files). • Skill in using Boolean operators to construct simple and complex queries. • Skill in tuning sensors. • Skill in physically disassembling PCs. • Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation. • Skill in conducting audits or reviews of technical systems. • Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems. • Skill in installing system and component upgrades. (i.e., servers, appliances, network devices). • Skill in monitoring and optimizing system/server performance. • Skill in recovering failed systems/servers. (e.g., recovery software, failover clusters, replication, etc.). • Skill in identifying gaps in technical delivery capabilities. • Skill in determining installed patches on various operating systems and identifying patch signatures. • Skill in server administration. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint). • Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). • Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud). • Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software). • Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. • Skill in writing test plans. • Skill in evaluating test plans for applicability and completeness.
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization’s data assets. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in creating and extracting important information from packet captures. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Abilities	
Category	**Ability**

Cybersecurity	• Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities. • Ability to prepare the final security assessment report containing the results and findings from the assessment. • Ability to recognize that changes to systems or environment can change residual risks in relation to risk appetite. • Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). • Ability to apply secure system design tools, methods and techniques. • Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). • Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). • Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat). • Ability to examine digital media on multiple operating system platforms.
Information Management	• Ability to analyse test data. • Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
Communication Networks	• Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware. • Ability to operate the organization's LAN/WAN pathways. • Ability to build architectures and frameworks. • Ability to design architectures and frameworks. • Ability to set up a physical or logical sub-networks that separates an internal local area network (LAN) from other untrusted networks. • Ability to operate common network tools (e.g., ping, traceroute, nslookup). • Ability to monitor traffic flows across the network. • Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity. • Ability to deploy continuous monitoring technologies and tools.
Personal Abilities	• Ability to effectively collaborate via virtual teams.

Substation Engineer

Table 39 contains a detailed a description of the Substation Engineer Role including assets, threats, knowledge, skills and abilities.

Table 39. Substation Engineer Role Description.

Role	Substation Engineer
Role	**Substation Engineer**

Role Description	The substation engineer is the responsible of the design of the transmission or distribution substations. The person in charge of configuring the electrical component of a substation. The substation engineer goes to the substation to program the protections and performs local test to assure their normal operations. Test to ensure the communication with the control centre are also performed.
Stakeholders	DSO, TSO
Location	Electrical Substations

Assets

Type	Category	Assets
Managed and controlled information	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators, etc., of substations
	Operational	Status, alarms, events, shortage, disturbances, etc., of the communication network.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Equipment Inventory (e.g., communication devices, IT servers, desktop, laptops, smart mobiles). Backup repository
	Applications	Asset Management System.
	Firmware	Firmware versions installed in the devices
Used services	Oriented to the staff	Mail, print service, authentication service.
	Oriented to the network	File service, network service, name service, address service.
Used hardware	Smart Grid, microgrid	RTU, IED, PLC, DCS
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point.
	Media devices	External storage
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	Substations

Threats & Vulnerabilities

Type	Category
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel). Erroneous use or administration of devices. Using information from an unreliable source (non-authorized firmware) Unintentional change of data in substation devices. Inadequate design or lack of adaptation
Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media. Information leakage that allow hackers to obtain private sensitive information: substation architecture, device information, user guides, …
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions

Nefarious Activity / Abuse	All threats should be considered.

Knowledge		
Category	**Level**	**Knowledge**
Collection	Basic	• Knowledge of collection disciplines and capabilities. • Knowledge of the available tools and applications associated with collection requirements and collection management.
Communication Networks	Basic	• Advanced knowledge about a communication technology
	Medium	• Basic knowledge about networks and communications • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
	Advanced	• Knowledge of the basic structure, architecture, and design of modern communication networks • Knowledge on network management • Knowledge about industrial and TCP/IP protocols
Cybersecurity	Basic	• Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities • Knowledge of cyber defense and information security policies, procedures, and regulations • Knowledge of ethical hacking principles and techniques • Knowledge of concepts and practices of processing digital forensic data • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
	Medium	• Knowledge of authentication, authorization, and access control methods • Knowledge of incident categories and incident responses
Information and Communication Technologies	Basic	• Knowledge of database management systems, query languages, table relationships, and views • Knowledge about the design and development of hardware devices • Knowledge of information technology (IT) architectural concepts and frameworks • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of the characteristics of physical and virtual data storage media • Knowledge of operating systems • Knowledge of computer programming principles • Knowledge of software design tools, methods, and techniques
	Advanced	• Knowledge of systems engineering theories, concepts, and methods
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization's data assets • Knowledge of data administration and data standardization policies
	Medium	• Knowledge of the capabilities and functionality associated with content creation and processing technologies
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures

Organisational	Advanced	• Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information • Knowledge of deconfliction processes and procedures • Knowledge of training and education policies, processes, and procedures • Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies
Technology Trend	Medium	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of emerging technologies that have potential for exploitation

Skills

Category	Skill
Cybersecurity	• Skill in assessing security systems designs. • Skill in translating operational requirements into protection needs (i.e., security controls). • Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles. • Skill in identifying critical target elements, to include critical target elements for the cyber domain.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyze that data). • Skill in developing data dictionaries. • Skill in developing data models. • Skill in recognizing relevance of information. • Skill in conducting information searches.

Abilities

Category	Ability
Cybersecurity	• Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations. • Ability to provide an assessment of the severity of weaknesses or deficiencies discovered in the system and its environment of operation and recommend corrective actions to address identified vulnerabilities. • Ability to prepare the final security assessment report containing the results and findings from the assessment. • Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Information and Communication Technologies	- Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	- Ability to evaluate information for reliability, validity, and relevance.
Personal Abilities	- Ability to effectively collaborate via virtual teams. - Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.

Substation Operator

Table 40 contains a detailed a description of the Substation Operator Role including assets, threats, knowledge, skills and abilities.

Table 40. Substation Operator Role Description.

Role	Substation Operator	
Role	**Substation Operator**	
Role Description	The person in charge of supervising the electrical components of a substation. Substation Operator is responsible to the normal function of the substation and coordinates with the grid operator to ensure power quality.	
Stakeholders	DSO, TSO	
Location	Electrical Substations	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators, etc., of substations.
	Operational	Status, alarms, events, shortage, disturbances, etc., of the communication network.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Substation device inventory (electrical and electronical) Backup repository
	Applications	Local SCADA/HMI. This SCADA is deployed in large substations to facilitate its supervision and control.
Used services	Oriented to the staff	Mail, print service, authentication service.
	Oriented to the network	File service, network service, name service, address service.
Used hardware	Smart Grid, microgrid	RTU, IED, PLC, DCS
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Media devices	External storage
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	Substations
Threats & Vulnerabilities		
Type	**Category**	
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel). Erroneous use or administration of devices. Unintentional operation in the substation.	

Damage/Loss (IT Assets)	Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media. Information leakage that allow hackers to obtain private sensitive information (e.g., substation architecture, device information, user guides).
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge		
Category	**Level**	**Knowledge**
Communication Networks	Basic	• Basic knowledge about networks and communications
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods • Knowledge of incident categories and incident responses • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
Information and Communication Technologies	Basic	• Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of systems engineering theories, concepts, and methods
Information Management	Basic	• Knowledge of data administration and data standardization policies • Knowledge of the capabilities and functionality associated with content creation and processing technologies
	Medium	• Knowledge of sources, characteristics, and uses of the organization’s data assets
Laws and Regulations	Medium	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Advanced	• Knowledge of organizational human resource policies, processes, and procedures. • Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies
Technology Trend	Medium	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of emerging technologies that have potential for exploitation

Skills	
Category	**Skill**
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.

Information and Communication Technologies	- Skill in generating queries and reports. - Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	- Skill to access information on current assets available, usage. - Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. - Skill in recognizing relevance of information. - Skill in conducting information searches.
Abilities	
Category	**Ability**
Cybersecurity	- Ability to understand the basic concepts and issues related to cyber and its organizational impact. - Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	- Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Personal Abilities	- Ability to effectively collaborate via virtual teams.

Installer

Table 41 contains a detailed a description of the Installer Role including assets, threats, knowledge, skills and abilities.

Table 41. Installer Role Description.

Role	**Installer**	
Role	**Installer**	
Role Description	Installing and maintaining of the electrical and electronic devices	
Stakeholders	DSO, TSO, manufacturer	
Location	Electrical Substations	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators, ... of substations.
	Operational	Status, alarms, events, shortage, disturbances, ... of the communication network.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Substation device inventory (electrical and electronical) Backup repository
	Applications	Local SCADA/HMI. This SCADA is deployed in large substations to facilitate its supervision and control.
	Operating Systems	Installed in the electronical devices
	Device Drivers	Installed in the electronical devices
	Firmware	Firmware versions installed in the devices
Used services	Oriented to the staff	Mail, print service, authentication service.
	Oriented to the network	File service, network service, name service, address service.

	Cloud services	Cloud repositories
Used hardware	Smart Grid, Microgrid	RTU, IED, PLC, DCS
	Servers	Hardware servers
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Network Components	Switch, router, bridge, repeater, modem, gateway, Firewall, WLAN access point.
	Media devices	External storage
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	Substations

Threats & Vulnerabilities	
Type	**Category**
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel). Erroneous use or administration of devices. Using information from an unreliable source Unintentional operation in the substation. Inadequate design or lack of adaptation
Damage/Loss (IT Assets)	Damage caused by a third party (in case the installer does not belong to the DSO/TSO) Loss of (integrity of) sensitive information, information device, storage media and documents. Destruction of records, devices or storage media. Information leakage that allow hackers to obtain private sensitive information (e.g., substation architecture, device information, user guides).
Failures/ Malfunction	Failure of devices or systems that can generate false positives of incidents. Failure or disruption of communication links when no secure protocols or standards are used.
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.

Knowledge		
Category	**Level**	**Knowledge**
Communication Networks	Medium	• Basic knowledge about networks and communications • Advanced knowledge about a communication technology • Knowledge on network management • Knowledge about industrial and TCP/IP protocols • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
	Advanced	• Knowledge of the basic structure, architecture, and design of modern communication networks
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods • Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities • Knowledge of cyber defense and information security policies, procedures, and regulations

		• Knowledge of cryptography and cryptographic key management concepts: encryption algorithms and methodologies • Knowledge of ethical hacking principles and techniques • Knowledge of concepts and practices of processing digital forensic data • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization • Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
Information and Communication Technologies	Basic	• Knowledge of how Internet applications work
	Medium	• Knowledge of database management systems, query languages, table relationships, and views • Knowledge about the design and development of hardware devices • Knowledge of information technology (IT) architectural concepts and frameworks • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of operating systems • Knowledge of software design tools, methods, and techniques
	Advanced	• Knowledge of the characteristics of physical and virtual data storage media • Knowledge of computer programming principles
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization's data assets • Knowledge of data administration and data standardization policies • Knowledge of the capabilities and functionality associated with content creation and processing technologies • Knowledge of critical information technology
Laws and Regulations	Medium	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures

Skills	
Category	**Skill**
Communication Networks	• Skill in using various open source data collection tools (online trade, DNS, mail, etc.). • Skill in analysing essential network data (e.g., router configuration files, routing protocols). • Skill in analysing traffic to identify network devices. • Skill in analysing network traffic capacity and performance characteristics. • Skill in diagnosing connectivity problems. • Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches. • Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). • Skill in using network management tools to analyse network traffic patterns (e.g., simple network management protocol). • Skill in using protocol analysers. • Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. • Skill in navigating network visualization software.

Cybersecurity	• Skill in recognizing and interpreting malicious network activity in traffic. • Skill in recognizing denial and deception techniques of the target. • Skill in system, network, and OS hardening techniques. (e.g., remove unnecessary services, password policies, network segmentation, enable logging, least privilege). • Skill in developing and deploying signatures. • Skill in using Virtual Private Network (VPN) devices and encryption. • Skill in reading and interpreting signatures (e.g., snort). • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). • Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles. • Skill in identifying critical target elements, to include critical target elements for the cyber domain.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files). • Skill in using Boolean operators to construct simple and complex queries. • Skill in tuning sensors. • Skill in physically disassembling PCs. • Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems. • Skill in installing system and component upgrades. (i.e., servers, appliances, network devices). • Skill in determining installed patches on various operating systems and identifying patch signatures. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint). • Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). • Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud). • Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software). • Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. • Skill in writing test plans. • Skill in evaluating test plans for applicability and completeness.
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization’s data assets. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in creating and extracting important information from packet captures. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Abilities	
Category	**Ability**
Cybersecurity	• Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). • Ability to understand the basic concepts and issues related to cyber and its organizational impact.

	• Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). • Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).
Information Management	• Ability to analyse test data. • Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
Communication Networks	• Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware. • Ability to operate common network tools (e.g., ping, traceroute, nslookup).
Personal Abilities	• Ability to effectively collaborate via virtual teams.

Prosumer

Table 42 contains a detailed a description of the Prosumer Role including assets, threats, knowledge, skills and abilities.

Table 42. Prosumer Role Description.

Role	Prosumer	
Role	**Prosumer**	
Role Description	Power generation at the point of consumption. Generating power on-site, rather than centrally, eliminates the cost, complexity, interdependencies, and inefficiencies associated with transmission and distribution. DIEL is a smart building with a Photovoltaic system installed on their roof, which will be controlled and monitored by the smart inverter and smart meters. Moreover, an energy storage system will be also installed (a proper size indoors battery) in order to store the excess amount of generated energy from the PV system. Every smart equipment of the DIEL building communicates with the smart network/meters installed in the building.	
Stakeholders	Prosumer	
Location		
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators.
	Operational	Status, alarms, events, shortage, disturbances, of the devices deployed at home.
	Historical information	Information that must be storage by law (e.g., supply contracts).
	Trending information	Information about the past that can be used to predict future generation and consumptions. It can be also used to select the energy supplier/aggregator.
	Trading information	Energy transactions, flexibility actions.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
	Databases:	Consumption and generation data repository (cloud).

Managed software	Applications	HEMS (Home Energy Management System) to supervise and control the generation, storage and consumption of energy and control de operation of the smart appliances.
Used services	Oriented to the staff	Mail, print service, authentication service.
	Cloud services	SaaS, IaaS
Used hardware	Microgrid	Smart Inverter, battery management system, central decision units, smart loads
	Smart Meter	End devices, local and neighbourhood network access point, external displays, home automation components, AMI head end.
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Network Components	Router, modem, firewall, VPN.
	Media devices	External storage
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	Building
eMobility	EV Charging Stations	EV charging post
	Vehicles	Electric vehicle

Threats & Vulnerabilities	
Type	**Category**
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel) Erroneous use or administration of devices Using information from an unreliable source Unintentional change of data in an information system Inadequate design or lack of adaptation
Damage/Loss (IT Assets)	Damage caused by a third party. Damages resulting from a penetration testing Loss of (integrity of) sensitive information, information device, storage media and documents. Loss of device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., bank accounts, smart meter control access, consumption habits).
Failures/ Malfunction	Failure of devices or systems Failure or disruption of communication links Failure or disruption of main supply Failure or disruption of service providers Malfunction of equipment Insecure Interfaces
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.
Outages	Lack of electricity Absence of personnel, strike, etc., of the supplier company (aggregator) Loss of support services Internet outage
Legal	Violation of laws or regulations / Breach of legislation

	Failure to meet contractual requirements Unauthorized use of copyrighted material

Knowledge		
Category	**Level**	**Knowledge**
Collection	Basic	• Knowledge of collection disciplines and capabilities.
Communication Networks	Basic	• Basic knowledge about networks and communications
Cybersecurity	Basic	• Knowledge of concepts and practices of processing digital forensic data • Knowledge of risk management processes • Knowledge of cybersecurity and privacy principles • Knowledge of cyber threats and vulnerabilities
	Medium	• Knowledge of authentication, authorization, and access control methods • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization
Information and Communication Technologies	Basic	• Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of operating systems
	Medium	• Knowledge about the design and development of hardware devices
Information Management	Basic	• Knowledge of critical information technology
	Medium	• Knowledge of sources, characteristics, and uses of the organization's data assets
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures

Skills	
Category	**Skill**
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.
Information and Communication Technologies	• Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in recognizing relevance of information.

Abilities	
Category	**Ability**
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Personal Abilities	• Ability to effectively collaborate via virtual teams.

Building Energy Manager

Table 43 contains a detailed a description of the Building Energy Manager Role including assets, threats, knowledge, skills and abilities.

Table 43. Building Energy Manager Role Description

Role	Building Energy Manager	
Role Description	Providing energy-related services to end-users.	
Stakeholders	ESCO	
Location	Office, Customer Building	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Cables, relays, transformers, power switches, sensors, actuators, etc., of the building.
	Operational	Status, alarms, events, shortage, disturbances, etc., of the devices deployed in the building.
	Historical information	Information that must be storage by law (e.g., supply contracts).
	Trending information	Information about the past that can be used to predict future generation and consumptions. It can be also used to select the energy supplier/aggregator.
	Trading information	Energy transactions, flexibility actions.
	System Configuration	Network topology, IP - MAC addresses, user credentials, permission, configuration files.
Managed software	Databases:	Consumption and generation data repository (cloud).
	Applications	HEMS (Home Energy Management System) to supervise and control the generation, storage and consumption of energy and control de operation of the smart appliances.
Used services	Oriented to the staff	Mail, print service, authentication service.
	Oriented to the network	File service, network service, name service, address service.
	Cloud services	SaaS, IaaS
Used hardware	Microgrid	Smart Inverter, battery management system, central decision units, smart loads
	Smart Meter	End devices, local and neighbourhood network access point, external displays, home automation components, AMI head end.
	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Network Components	Router, modem, firewall, VPN.
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	Building
	Power	Transformer Emergency Generator, UPS.
	Air Conditioning	
eMobility	EV Charging Stations	EV charging post
Threats & Vulnerabilities		
Type	**Category**	

Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel) Erroneous use or administration of devices Using information from an unreliable source Unintentional change of data in an information system Inadequate design or lack of adaptation
Damage/Loss (IT Assets)	Damage caused by a third party. Damages resulting from a penetration testing Loss of (integrity of) sensitive information, information device, storage media and documents. Loss of device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., bank accounts, smart meter control access, consumption habits).
Failures/ Malfunction	Failure of devices or systems Failure or disruption of communication links Failure or disruption of main supply Failure or disruption of service providers Malfunction of equipment Insecure Interfaces
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.
Outages	Lack of electricity Absence of personnel, strike. Loss of support services Internet outage
Legal	Violation of laws or regulations / Breach of legislation Failure to meet contractual requirements Unauthorized use of copyrighted material

Knowledge

Category	Level	Knowledge
Collection	Advanced	• Knowledge of collection management processes, capabilities, and limitations. • Knowledge of collection disciplines and capabilities. • Knowledge of the available tools and applications associated with collection requirements and collection management.
Communication Networks	Medium	• Basic knowledge about networks and communications
Cybersecurity	Basic	• Knowledge of incident categories and incident responses
	Advanced	• Knowledge of authentication, authorization, and access control methods
Information and Communication Technologies	Basic	• Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of operating systems
	Advanced	• Knowledge about the design and development of hardware devices

Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization's data assets • Knowledge of the capabilities and functionality associated with content creation and processing technologies • Knowledge of critical information technology
	Medium	• Knowledge of data administration and data standardization policies
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Basic	• Knowledge of organizational human resource policies, processes, and procedures. • Knowledge of organizational process improvement concepts and process maturity models • Knowledge about company organizational structure, roles and responsibilities
	Medium	• Knowledge of intelligence disciplines
Technology Trend	Basic	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of emerging technologies that have potential for exploitation

Skills

Category	Skill
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill to access information on current assets available, usage. • Skill to identify sources, characteristics, and uses of the organization's data assets. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in conducting social network analysis. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	• Skill in complying with the legal restrictions for targeted information.
Organisational	• Skill to compare indicators/observables with requirements. • Skill to craft indicators of operational progress/success.

Abilities

Category	Ability
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Information Management	• Ability to evaluate information for reliability, validity, and relevance.

Laws and Regulations	• Ability to author a privacy disclosure statement based on current laws.
Personal Abilities	• Ability to effectively collaborate via virtual teams.

Developer

Table 44 contains a detailed a description of the Developer Role including assets, threats, knowledge, skills and abilities.

Table 44. Developer Role Description

Role	**Developer**	
Role Description	Developing and providing hardware and software components and solutions	
Stakeholders	Hardware y Software Providers.	
Location	Own Premises, Customer Building	
	Assets	
Type	**Category**	**Assets**
Managed and controlled information		
Managed software	Databases:	Copy of customer databases
	Applications	IDE (Integrated Development Environments).
	Operating Systems	
	Device Drivers	
	Firmware	
Used services	Oriented to the staff	Mail, print service, authentication service, …
	Oriented to the network	File service, network service, name service, address service.
	Cloud services	SaaS, IaaS
Used hardware	Smart Grid,	RTU, IED, PLC, DCS,
	Microgrid	Smart Inverter, battery management system, central decision units, smart loads
	Smart Meter	End devices, local and neighbourhood network access point, external displays, home automation components, AMI head end.
	Servers	Hardware servers
	Clients	PC, Notebook, Tablet, mobile-phone, printer, ...
	Network Components	Router, modem, firewall, VPN.
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	When working in the customer facilities
	Threats & Vulnerabilities	
Type	**Category**	
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel) Erroneous use or administration of devices Using information from an unreliable source Unintentional change of data in an information system Inadequate design or lack of adaptation	

Damage/Loss (IT Assets)	Damage caused by a third party. Damages resulting from a penetration testing Loss of (integrity of) sensitive information, information device, storage media and documents. Loss of device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information (e.g., bank accounts, smart meter control access, consumption habits).
Failures/ Malfunction	Failure of devices or systems Failure or disruption of communication links Failure or disruption of main supply Failure or disruption of service providers Malfunction of equipment Insecure Interfaces
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions
Nefarious Activity / Abuse	All threats should be considered.
Outages	Lack of electricity Absence of personnel, strike. Loss of support services Internet outage
Legal	Violation of laws or regulations / Breach of legislation Failure to meet contractual requirements Unauthorized use of copyrighted material

Knowledge		
Category	**Level**	**Knowledge**
Collection	Basic	• Knowledge of collection disciplines and capabilities.
Communication Networks	Medium	• Basic knowledge about networks and communications • Advanced knowledge about a communication technology • Knowledge of the basic structure, architecture, and design of modern communication networks
	Advanced	• Knowledge on network management • Knowledge about industrial and TCP/IP protocols • Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware
Cybersecurity	Basic	• Knowledge of what constitutes a network attack and a network attack’s relationship to both threats and vulnerabilities • Knowledge of cyber defense and information security policies, procedures, and regulations • Knowledge of cryptography and cryptographic key management concepts: encryption algorithms and methodologies • Knowledge of concepts and practices of processing digital forensic data • Knowledge of incident categories and incident responses • Knowledge of cybersecurity and privacy principles

		• Knowledge of cyber threats and vulnerabilities
	Medium	• Knowledge of authentication, authorization, and access control methods • Knowledge of ethical hacking principles and techniques • Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization
Information and Communication Technologies	Basic	• Knowledge about the design and development of hardware devices • Knowledge of information technology (IT) architectural concepts and frameworks • Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly • Knowledge of the characteristics of physical and virtual data storage media • Knowledge of operating systems
	Advanced	• Knowledge of database management systems, query languages, table relationships, and views • Knowledge of computer programming principles • Knowledge of software design tools, methods, and techniques • Knowledge of how Internet applications work
Information Management	Basic	• Knowledge of the capabilities and functionality associated with content creation and processing technologies
	Medium	• Knowledge of data administration and data standardization policies
Organisational	Advanced	• Knowledge of training and education policies, processes, and procedures • Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies
Technology Trend	Basic	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of machine learning theory and principles

Skills	
Category	**Skill**
Communication Networks	• Skill in using various open source data collection tools (online trade, DNS, mail, etc.). • Skill in analysing essential network data (e.g., router configuration files, routing protocols). • Skill in analysing network traffic capacity and performance characteristics. • Skill in diagnosing connectivity problems. • Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches. • Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). • Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. • Skill in extracting information from packet captures. • Skill in navigating network visualization software.
Cybersecurity	• Skill in designing multi-level security/cross domain solutions. • Skill in developing and deploying signatures. • Skill in using Virtual Private Network (VPN) devices and encryption.

	• Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]). • Skill in reading and interpreting signatures (e.g., snort). • Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). • Skill in assessing the application of cryptographic standards. • Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.). • Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles. • Skill in designing security controls based on cybersecurity principles and tenets.
Information and Communication Technologies	• Skill in generating queries and reports. • Skill in maintaining databases. (i.e., backup, restore, delete data, transaction log files, etc.). • Skill in optimizing database performance. • Skill in exploiting/querying organizational and/or partner collection databases. • Skill in using Boolean operators to construct simple and complex queries. • Skill in using databases to identify target-relevant information. • Skill in using targeting databases and software packages. • Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation. • Skill in systems integration testing. • Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems. • Skill in installing system and component upgrades. (i.e., servers, appliances, network devices). • Skill in determining installed patches on various operating systems and identifying patch signatures. • Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint). • Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). • Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.). • Skill in operating system administration. (e.g., account maintenance, data backups, maintain system performance, install and configure new hardware/software). • Skill in writing code in a currently supported programming language (e.g., Java, C++). • Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode). • Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc. • Skill in using code analysis tools. • Skill in analysing language processing tools to provide feedback to enhance tool development. • Skill in interpreting compiled and interpretive programming languages. • Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data). • Skill in relevant programming languages (e.g., C++, Python, etc.).

	• Skill in remote command line and Graphic User Interface (GUI) tool usage. • Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools. • Skill in applying secure coding techniques. • Skill in conducting software debugging. • Skill in conducting test events. • Skill in configuring and optimizing software. • Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams. • Skill in developing operations-based testing scenarios. • Skill in design modelling and building use cases (e.g., unified modelling language). • Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. • Skill in writing test plans. • Skill in evaluating test plans for applicability and completeness. • Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures. • Skill in the use of design methods. • Skill in secure test plan design (e. g. unit, integration, system, acceptance). • Skill in the use of design modelling (e.g., unified modelling language). • Skill in applying the systems engineering process.
Information Management	• Skill in using data mapping tools. • Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches. • Skill in designing a data analysis structure (i.e., the types of data a test must generate and how to analyse that data). • Skill in developing data dictionaries. • Skill in developing data models. • Skill in analysing volatile data. • Skill in reading Hexadecimal data. • Skill in data pre-processing (e.g., imputation, dimensionality reduction, normalization, transformation, extraction, filtering, smoothing). • Skill in performing format conversions to create a standard representation of the data. • Skill in developing machine understandable semantic ontologies. • Skill in analysing terminal or environment collection data. • Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis. • Skill in evaluating and interpreting metadata. • Skill in recognizing relevance of information. • Skill in conducting information searches.
Laws and Regulations	•
Technology Trends	• Skill in creating and utilizing mathematical or statistical models. • Skill in using scientific rules and methods to solve problems. • Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS). • Skill to remain aware of evolving technical infrastructures.
Abilities	
Category	**Ability**

Cybersecurity	• Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth). • Ability to apply secure system design tools, methods and techniques. • Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to maintain databases. (e.g., backup, restore, delete data, transaction log files). • Ability to optimize systems to meet enterprise performance requirements. • Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts). • Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat). • Ability to examine digital media on multiple operating system platforms. • Ability to apply programming language structures (e.g., source code review) and logic. • Ability to develop secure software according to secure software deployment methodologies, tools, and practices. • Ability to employ best practices when implementing security controls within a system including software engineering methodologies; system and security engineering principles; secure design, secure architecture, and secure coding techniques. • Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools. • Ability to execute technology integration processes. • Ability to interpret and translate customer requirements into operational capabilities.
Information Management	• Ability to analyse test data. • Ability to build complex data structures and high-level programming languages. • Ability to collect, verify, and validate test data. • Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
Communication Networks	• Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware. • Ability to operate common network tools (e.g., ping, traceroute, nslookup).
Personal Abilities	• Ability to effectively collaborate via virtual teams.

IT User

Table 45 contains a detailed a description of the IT User Role including assets, threats, knowledge, skills and abilities.

Table 45. IT User Role Description

Role	IT Users
Role Description	We include in this role all those company personnel who perform a support function for the other roles defined above.
Stakeholders	All

Location	Office	
Assets		
Type	**Category**	**Assets**
Managed and controlled information	Inventory of Electrical Assets	Depending on the department in which each person works, they have access to information of a different nature.
	Operational	
	Historical information	
	Trending information	
	Trading information	
	System Configuration	
Managed software	Databases:	IT user, depending on its responsibility, can access to different types of applications and databases can be accessed. Currently, there is a tendency to upload all the company's information to servers and repositories in the cloud.
	Applications	
Used services	Oriented to the staff	Mail, print service, authentication service.
	Oriented to the network	File service, network service, name service, address service.
	Cloud services	SaaS, IaaS
Used hardware	Clients	PC, Notebook, Tablet, mobile-phone, printer.
	Media devices	External storage
	Displays	Monitor, Beamer
	Human interaction	Keyboard, mouse
Infrastructure	Facilities	Premises, buildings, office.
Threats & Vulnerabilities		
Type	**Category**	
Unintentional damage (accidental)	Information leakage / sharing due to user error (credential steel) Using information from an unreliable source Unintentional change of data in an information system	
Damage/Loss (IT Assets)	Damage caused by a third party. Loss of (integrity of) sensitive information, information device, storage media and documents. Loss of device, storage media and documents. Destruction of records, devices or storage media, for example because of a ransomware attack. Information leakage that allow hackers to obtain private sensitive information	
Failures/ Malfunction	Failure or disruption of communication links Failure or disruption of main supply Failure or disruption of service providers Malfunction of equipment Insecure Interfaces	
Eavesdropping / Interception / Hijacking	Interception of information Replay of messages Network reconnaissance and information gathering Man in the Middle / Session hijacking Repudiation of actions	
Nefarious Activity / Abuse	All threats should be considered.	
Outages	Lack of resources Lack of electricity Absence of personnel, strike. Loss of support services	

	Internet outage Network outage
Legal	Violation of laws or regulations / Breach of legislation Failure to meet contractual requirements Unauthorized use of copyrighted material

Knowledge		
Category	**Level**	**Knowledge**
Collection	Basic	• Knowledge of collection management processes, capabilities, and limitations. • Knowledge of collection disciplines and capabilities. • Knowledge of the available tools and applications associated with collection requirements and collection management.
Communication Networks	Basic	• Basic knowledge about networks and communications • Advanced knowledge about a communication technology
Cybersecurity	Basic	• Knowledge of authentication, authorization, and access control methods
Information and Communication Technologies	Basic	• Knowledge of database management systems, query languages, table relationships, and views
Information Management	Basic	• Knowledge of sources, characteristics, and uses of the organization’s data assets • Knowledge of data administration and data standardization policies
Laws and Regulations	Basic	• Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures
Organisational	Basic	• Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information • Knowledge of organizational human resource policies, processes, and procedures. • Knowledge of intelligence disciplines • Knowledge of organizational process improvement concepts and process maturity models • Knowledge about company organizational structure, roles and responsibilities • Knowledge of organizational security policies
Technology Trend	Medium	• Knowledge of successful capabilities to identify the solutions to less common and more complex system problems: computer algorithms, mathematics • Knowledge of machine learning theory and principles • Knowledge of emerging technologies that have potential for exploitation

Skills	
Category	**Skill**
Cybersecurity	• Skill in performing impact/risk assessments. • Skill in applying confidentiality, integrity, and availability principles.
Information and Communication Technologies	• Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
Information Management	• Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.

	• Skill in recognizing relevance of information.
Abilities	
Category	**Ability**
Cybersecurity	• Ability to understand the basic concepts and issues related to cyber and its organizational impact. • Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Information and Communication Technologies	• Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
Personal Abilities	• Ability to effectively collaborate via virtual teams.