

# **RESISTO:**

## **D2.1\_End user requirements for integrated cyber-physical risk and resilience management, platform and tools**



# RESISTO

## D2.1 – END USER REQUIREMENTS FOR INTEGRATED CYBERPHYSICAL RISK AND RESILIENCE MANAGEMENT, PLATFORM AND TOOLS

<b>Document Manager:</b>	Sylvia Bach	BUW	Editor
--------------------------	-------------	-----	--------

<b>Project Title:</b>	RESilience enhancement and risk control platform for communication infraSTructure Operators
<b>Project Acronym:</b>	RESISTO
<b>Contract Number:</b>	786409
<b>Project Coordinator:</b>	LEONARDO
<b>WP Leader:</b>	BTC

<b>Document ID N°:</b>	RESISTO_D2.1_190507_05	<b>Version:</b>	5.0
<b>Deliverable:</b>	D2.1	<b>Date:</b>	07/05/2019
		<b>Status:</b>	APPROVED

<b>Document classification</b>	<b>PUBLIC</b>
--------------------------------	---------------

Approval Status	
<b>Prepared by:</b>	Sylvia BACH (BUW)
<b>Approved by: (WP Leader)</b>	Zhan CUI (BTC)
<b>Approved by: (Coordinator)</b>	Federico FROSALI (LDO)
<b>Advisory Board Validation (Advisory Board Coordinator)</b>	Carmen PATRASCU (ORO)
<b>Security Approval (Security Advisory Board Leader)</b>	NA

## CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Alberto Neri	LDO	Contributor
Marco Carli	RM3	Contributor
Carmen Patrascu	ORO	Contributor
Ioan Constantin	ORO	Contributor
Jorge Carapinha	ALB	Contributor
Luis Moreno	RTV	Contributor
Maria Belesioti	OTE	Contributor
Rodoula Makri	ICCS	Contributor
Panos Karaivazoglou	ICCS	Contributor
Apostolos Papafragkakis	ICCS	Contributor
Athanasios Panagopoulos	ICCS	Contributor
Panagiotis Fragkos	ICCS	Contributor
Eyangelos Groumpas	ICCS	Contributor
Michalis Sofras	ICCS	Contributor
Takis Kelefas	ICCS	Contributor
Luca Lionetti	TIM	Contributor
Moises Valeo	INT	Contributor
Javier Valera	INT	Contributor
Jose Sanchez	INT	Contributor
Zhan Cui	BTC	Contributor
Selina Wang	BTC	Contributor
Ian Herwono	BTC	Contributor
Mirjam Fehling-Kaschek	EMI	Contributor

## DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

## REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
2.0	22.3.2019	approx. 20		By task contributors
3.0	26.03.2019			By WP leader
4.0	29.03.2019	All	ALL	Final release for AB approval
5.0	07.05.2019	All	ALL	Final release

## COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISSO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

## PROJECT CONTACT



LEONARDO

Via delle Officine Galileo 1 – Campi Bisenzio (FI) –  
50013 – Italy

Tel.: +39 055 5369640, Fax: +39 055 5369640

E-Mail: frederico.frosali@leonardocompany.com

## RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

## EXECUTIVE SUMMARY

To ensure that the RESISTO platform meets the end users' needs, this deliverable summarizes both the security requirements captured from the consortium members via questionnaires and comprehensive requirements extracted from literature on past events. In addition, a literature research on the feelings of (in)security during major disruptions has been carried out to include a societal view on the topic.

One of the important outcomings of the process of developing this deliverable has been the setting of the structure and classification of requirements (see chapter 4) that all end user members of the consortium agreed on. The collected and structured requirements can now be used as a guideline for the design of the RESISTO platform.

The method of collecting information from the consortium members via questionnaires has been found to be a challenging one. The variety of security issues – from user to system, physical to cyber, design to performance etc. – come with the same variety of responsible persons and departments. Chapter 3 describes the method and analyses the received questionnaires. Some of the results are crucial for the development of the RESISTO platform, such as the factors that determine if a risk is acceptable or not.

With the answers to these questions and the comprehensive list of requirements the operators have regarding the platform, this document provides the basis for the system engineering process of the RESISTO platform.

## CONTENTS

<b>ABBREVIATIONS .....</b>	<b>10</b>
<b>1. INTRODUCTION .....</b>	<b>13</b>
<b>2. Objective and scopes .....</b>	<b>14</b>
<b>3. Interaction with other project tasks .....</b>	<b>15</b>
<b>4. Requirements elicitation methodology .....</b>	<b>16</b>
4.1. Requirement types .....	16
4.2 Requirement identification .....	17
4.3 Requirement enunciation .....	18
4.4 Requirement verifiability .....	19
<b>5. Expert input and societal impact .....</b>	<b>20</b>
5.1 Vulnerabilities of the telecommunication infrastructure .....	20
5.2 Societal impact of disruptions .....	24
5.3 Input from operators and technical experts .....	27
5.3.1. Context Analysis .....	27
5.3.2. System Analysis .....	29
5.3.3. System Performance Function Identification .....	30
5.3.4. Disruption Identification .....	31
5.3.5. Pre-Assessment of the criticality of System Functions and Disruptions .....	32
5.3.6. Overall Resilience Quantification .....	34
5.3.7. Resilience Evaluation / Risk Acceptance / Decision Making .....	34
5.3.8. Selection of Options to improve Resilience Development and Implementation .....	34
5.3.9. Development and Implementation of Options improving Resilience .....	35
<b>6. Requirements .....</b>	<b>36</b>
<b>6.1 Functional Requirements .....</b>	<b>36</b>
6.1.1. Input Data .....	38
6.1.2. System Work-Flows .....	39
6.1.3 Vulnerability Disclosure .....	39
6.1.4. System Reports and other Output .....	40
6.1.5. Data Input Permission .....	40
6.1.6. Functional Requirements related to 5G .....	41
<b>6.2 Non-Functional Requirements .....</b>	<b>41</b>
6.2.1. Design Requirements .....	41
6.2.2. Implementation Requirements .....	41
6.2.3. Interface Requirements .....	42
6.2.4. Security Requirements .....	43
6.2.5. Operating Requirements .....	48



6.3 Mandatory Requirements .....	48
7. REFERENCES .....	52
ANNEX 1 .....	53

## ABBREVIATIONS

<b>3GPP</b>	3 <sup>rd</sup> Generation Partnership Project
<b>5G</b>	Fifth generation of mobile phone systems
<b>AI</b>	Artificial Intelligence
<b>API</b>	Application Programming Interface
<b>BGP</b>	Border Gateway Protocol
<b>BYOD</b>	Bring Your Own Device
<b>CCTV</b>	Closed Circuit Television
<b>CERT</b>	Computer Emergency Response Team
<b>CI</b>	Critical Infrastructure
<b>CRM</b>	Customer Relationship Management
<b>COPE</b>	Company Owned, Personally Enabled
<b>CSIRT</b>	Computer Security Incident Response Team
<b>CVS</b>	Comma Separated Values
<b>DaaS</b>	Device as a Service
<b>DDoS</b>	Distributed Denial of Services
<b>DMO</b>	Direct Mode Operations
<b>DoW</b>	Description of Work
<b>EGP</b>	Exterior Gateway Protocol
<b>ENISA</b>	European Union Agency for Network and Information Security
<b>ETSI</b>	European Telecommunications Standard Institute
<b>EU</b>	European Union
<b>FTP</b>	File Transfer Protocol
<b>GDPR</b>	General Data Protection Regulation
<b>GLBP</b>	Gateway Load Balancing Protocol
<b>HSRP</b>	Hot Standby Router Protocol
<b>HW</b>	Hardware
<b>IaaS</b>	Infrastructure as a Service
<b>ICD</b>	Industrial Control Devices

<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IGP</b>	Interior Gateway Protocol
<b>IoT</b>	Internet of Things
<b>IPSec</b>	Internet Protocol SECurity
<b>ISO</b>	International Standardization Organization
<b>IT</b>	Information Technology
<b>ITU</b>	International Telecommunication Union
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MANO</b>	NFV Management and Network Orchestration
<b>MACSEC</b>	Media Access Control Security
<b>MSAD</b>	Microsoft Active Directory
<b>MSSP</b>	Managed Security Service Provider
<b>NFV</b>	Network Function Virtualization
<b>NGFW</b>	Next Generation Firewall
<b>OS</b>	Operating System
<b>PaaS</b>	Platform as a Service
<b>POCE</b>	Personally Owned, Company Enabled
<b>RBAC</b>	Role Based Access Control
<b>SaaS</b>	Software as a Service
<b>SCP</b>	Secure Copy Protocol
<b>SIEM</b>	Security Information and Event Management
<b>SOC</b>	Security Operations Center
<b>SSL</b>	Secure Sockets Layer
<b>SSN</b>	Social Security Number
<b>SSO</b>	Single Sign On
<b>SysML</b>	Systems Modelling Language
<b>SW</b>	Software
<b>TLC</b>	Telecommunications
<b>TRL</b>	Technical Readiness Level
<b>VPN</b>	Virtual Private Network

<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>WP</b>	Work Package
<b>XLS</b>	Excel file extension
<b>XML</b>	Extensible Markup Language

## 1. INTRODUCTION

To construct an expert platform useful and practical for telecommunication providers throughout Europe - with different operation procedures, network structures and also some individual threats they face - it is essential to gain a broad understanding of the topic of everyday threats these organisations cope with, as well as (real and potential) serious threats they are preparing for.

The aim of WP2 is the refinement and specification of user expectations and requirements for the RESISTO platform. It was designed to collect the necessary inputs for the implementation of the tools and methods throughout the other work packages. The following tasks are included in WP2:

Task 2.1 Communication operators requirements refinement

Task 2.2 Cyber physical threat, hazard and disruption ranking ontology

Task 2.3 Holistic socio-technical communication infrastructure system modelling

Task 2.4 RESISTO reference architecture for long term preparation and short term disruptions

Task 2.5 Operational use cases and validation plan

This report summarizes the status and results of task 2.1.

After laying out the scope and objective of the task (chapter 2), an overview of the tasks within the RESISTO project that interact with this document and the methods and results behind is given in chapter 3. Chapter 4 describes the elicitation methodology and the chosen nomenclature for the requirements.

In chapter 5, method and results of questionnaires completed by the end users/telecommunication operators of the consortium and other technical experts are elaborated on as well as the societal impact of disruptions in telecommunication infrastructure failures. With relevant research and annual reports from organisations (e.g. the “Annual incident reports” by the European Union Agency for Network and Information Security (ENISA)) an overview is given of the state of the art of the vulnerabilities both the operators and their customers face.

The complete requirements collected from the operators and other technical experts in the RESISTO consortium necessary for the advancement of the project are listed and explained in chapter 6.

Those requirements mandatory for the project phase of the RESISTO platform (TRL 7) are listed again separately in subchapter 6.3.

## 2. OBJECTIVE AND SCOPES

The objective of this document is to derive requirements for the RESISTO framework and with that to provide a knowledge base for the overall system architecture.

The requirements will define the scope of the project and the RESISTO system. They will be used as a guideline for the technical developments to be carried out and will provide an objective means of validation and verification of the project's results.

Requirements and specifications are collected based on expert and stakeholder judgement, and, particularly, the end users of the project consortium via questionnaires, conference calls and E-Mails. Preliminary discussions of simple use cases, the state of the art regarding some security issues, technical standards and the relevant pilot or research project experiences (CockpitCI and ATENA) resulted in a broad and comprehensive overview of the requirements.

According to the ITU [ITU2015], a comprehensive review of security requirements must take the following into account:

- The parties involved
- The assets that need to be protected
- The threats against which those assets must be protected
- The vulnerabilities associated with the assets and the environment
- The overall risk to the assets deriving from those threats and vulnerabilities

The requirements collected for this report are following this, providing very detailed descriptions of potential and mandatory features the RESISTO platform has to have in order to be useful and valuable for its end users.

### 3. INTERACTION WITH OTHER PROJECT TASKS

The definition of the system requirements is the very first step in a system engineering process. Therefore, task 2.1 and its deliverable D2.1 are related to all the following system engineering phases that are and will be part of the RESISTO project:

- System design (architecture definition); T2.4, T6.1
- System components design and development; T3.1, T4.3, T4.4, T5.2, T5.3, T5.4, T5.5, T6.2, T6.4
- System integration and tests; T6.3, T6.5
- System validation; WPs 7, 8, 9

This document must also be put into context with T2.2 and the resulting deliverables D2.2 and D2.3, because the threats and hazards communication infrastructure providers face are directly related to a lot of the system requirements. Both these threats and hazards and the requirements have been collected from the consortium members that are telco infrastructure providers, partly in the same questionnaire (see annex 1) and partly separately.

## 4. REQUIREMENTS ELICITATION METHODOLOGY

This section reports the methodology adopted in task 2.1 to define the requirements related to the RESISTO system. In the following, the type of requirements, the adopted notation and the requirement code conventions are described.

### 4.1 Requirement types

Requirement definitions that have been adopted in this document are aligned with the relevant IEEE Standard Glossary of Software Engineering Terminology [Ref2].

Accordingly, a requirement is defined as followed:

- “(1) A condition or capability needed by a user to solve a problem or achieve an objective.
- (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents.
- (3) A documented representation of a condition or capability as in (1) and (2)”.

RESISTO system requirements are classified as functional or non-functional requirements:

- **Functional Requirement:** a requirement that specifies a function that a system, or system component, must be able to perform. A requirement specifying **what** the overall system, or a specific component, will be able to do. Statements of services that the system should provide, how the system should react to particular inputs and how the system should behave in particular situations. Among the functional requirements are also included security requirements relating to the security services offered by the system to users or other systems.
- **Non-functional Requirement:** a requirement specifying **how** the system or component will implement its functionality. In this document the following non-functional types of requirements are considered:
  - **Design Requirement:** a requirement that specifies or constraints the design of a system or system component. A design constraint requirement defines the limits on the options of a solution that are available to a designer; for example, to use a specific technology, product or the adoption of a specific technical standard.
  - **Implementation Requirement:** a requirement that specifies or constrains the coding or construction of a system or system component.
  - **Interface Requirement:** a requirement that specifies an external item with which a system or system component must interact, or that sets forth constraints on formats, timing, or other factors caused by such an interaction.
  - **Security Requirement:** a requirement specifying security-related aspects, that is how the system secures itself (security functions that the system provides to users or other systems or infrastructures are to be considered functional requirements).
  - **Operating Requirement:** a requirement defining the operational conditions or properties that are required for the system to operate or exist. This type of requirement includes: human factors, ergonomics, availability, maintainability, reliability.



## 4.2 Requirement identification

The RESISTO system requirements will be uniquely identified by an alphanumeric code consisting of:

<project>\_<classification>\_<number>

where:

- the RESISTO <project> is identified by the abbreviation **RES**;
- the requirement <classification> is indicated with:
  - **FUN** for a Functional Requirement,
  - **DCC** for a Design Requirement,
  - **IMP** for an Implementation Requirement,
  - **INT** for an Interface Requirement,
  - **SEC** for a Security Requirement,
  - **OPR** for an Operating Requirement.
- <number> is a progressive number that uniquely identifies the classified requirement. A step 10 is usually used in order to allow requirements insertion during successive reviews.

The different codes for identifying requirements are thus illustrated in the following table.

CLASSIFICATION	CATEGORY
Functional	RES_ FUN_<num>
Design	RES_ DCC_<num>
Implementation	RES_ IMP_<num>
Interface	RES_ INT_<num>
Security	RES_ SEC_<num>
Operational	RES_ OPR_<num>

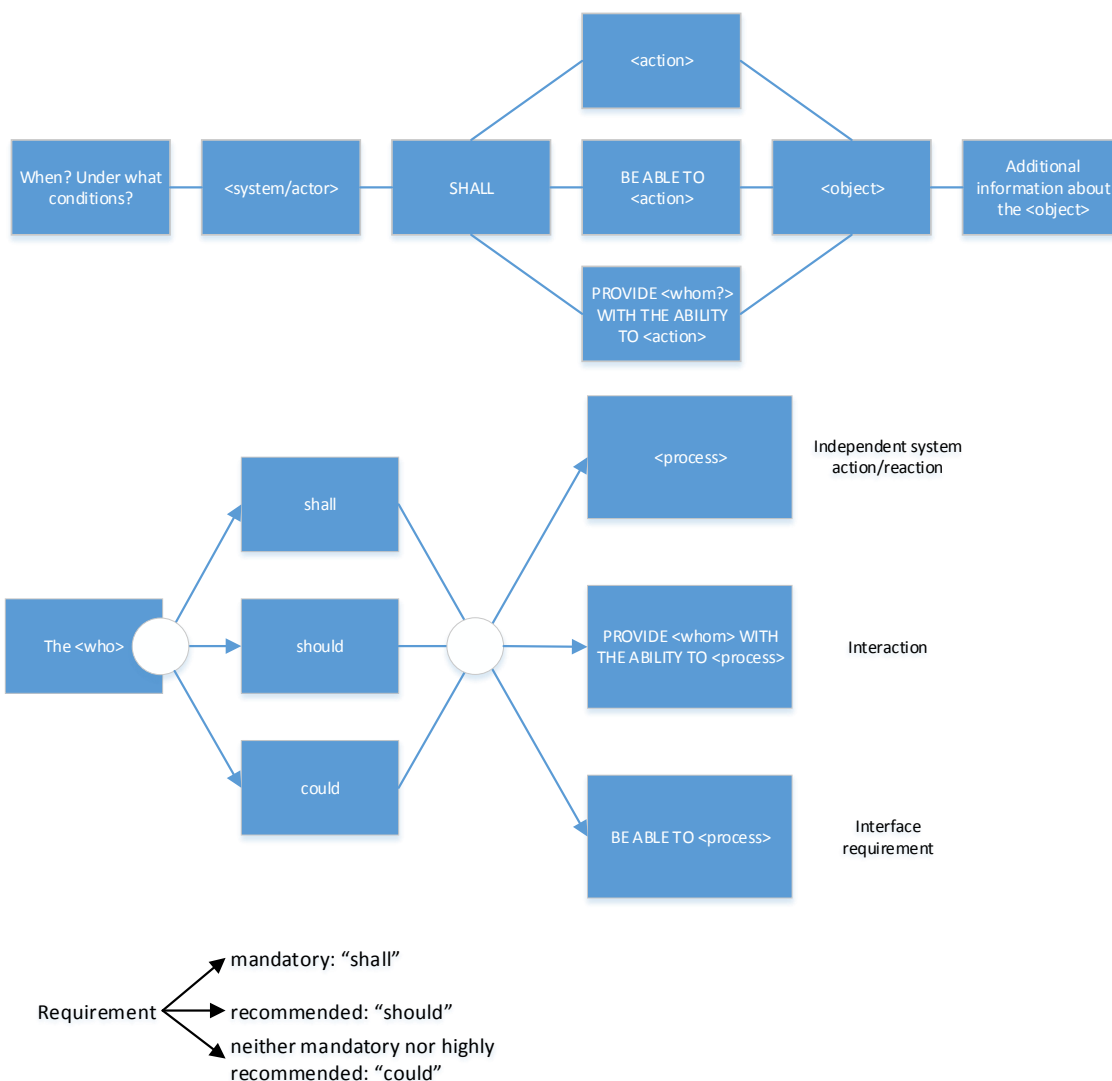
Table 1 - RESISTO requirement identity codes

### 4.3 Requirement enunciation

Each requirement should be:

- **UNAMBIGUOUS:** a requirement should not be able to have multiple interpretations;
- **CONSISTENT:** a requirement should haven't conflicts or contradictions in own description and two requirements should not contradict each other;
- **REALISTIC:** a requirement can be implemented within constraints;
- **VERIFIABLE:** a requirement is verifiable if there exists some finite cost-effective process with which a person or machine can check that the system meets the requirement. In general any ambiguous requirement isn't verifiable.

The requirements are structured as sentences and follow, where possible, a fixed pattern:



<who>: object for which the requirement is written (e.g. system, component, function,...)

<process>: activities/actions to be described (e.g. 'display...', 'activate...')

<whom>: an actor (e.g. a user or another system)

Figure 1 - Fixed pattern for the structure of requirements / requirement sentence

---

where the words **shall**, **should** and **could** are used as follows:

- **Shall:** to indicate mandatory requirements to be fulfilled in order to achieve the system objectives such as the DoW target of TRL level 7 “System prototyping demonstration in an operational environment”.
- **Should:** the implementation of such requirements is recommended if and when the RESISTO platform will be completed and run in a production environment (TRL 8 and 9, after the project phase).
- **Could:** to refer to “nice to have” requirements, whose implementation is not mandatory, nor highly recommended, but would be useful to improve the platform.

#### 4.4 Requirement verifiability

Each requirement shall be verifiable with at least one of the following methods:

- **Test (T):** verification of measurable functional characteristics, which can be accessed directly or indirectly. Standard or special test equipment could be required.
- **Demonstration (D):** verification of the operational characteristic observable on the system components in operation, without involving physical measurements. Examples: demonstration of a start-up sequence, the operation of a safety circuit, operation of an integrated test device, etc.
- **Inspection (I):** visual or dimensional verification of system components. Verification is based on the human senses (sight, touch) or else uses simple measurement and handling methods. No stimulus is necessary. Passive resources such as a metre rule, microscope, gauge, etc. can be used.
- **Analysis (A):** verification based on analytic proofs obtained by calculation, without any intervention on the system components. The techniques used are modelling, simulation and prediction.

Functional requirements are mainly verified by Testing or Demonstration. At this stage of the project, not all requirements could be assigned to a verification method yet and some might have to be changed during the course of the project.

## 5. EXPERT INPUT AND SOCIETAL IMPACT

One of the biggest challenges of our times is the adaption of communities to extreme weather conditions [NRC2014]. Policy and decision makers need to change the way of managing hazards from reactive to proactive – enhancing community resilience systematically [BER2018].

Another problem is cyber security. Cyberattacks become more sophisticated with increasing computational powers. Industries often have the feeling of being one step behind the attackers. In Germany, cybercrime has gone up from 59.900 cases in 2010 to 86.000 in 2017 [BKA2010, 2017], an increase of almost 44 %.

Critical infrastructures are one of the biggest assets in a community and vital for a functioning society. Their vulnerabilities are at the same time vulnerabilities of a community. And within those critical infrastructures (CIs), telecommunication infrastructures have become more and more important, because almost all other critical infrastructures such as the power and water supply or the transportation and finance sectors rely on network systems using data transmission of any kind. This also applies to the people within a society.

This chapter tries to provide an overview of the state of the art of the vulnerabilities both the operators of telecommunication services (subchapter 5.1) and their customers (subchapter 5.2) face. Identifying vulnerabilities will help to evaluate the requirements that are being defined in Chapter 6 and put them into the right perspective.

Subchapter 5.3 summarizes the results of the questionnaire the end user consortium members completed. The whole questionnaire and its anonymized results can be found in annex 1.

### 5.1 Vulnerabilities of the telecommunication infrastructure

The ENISA (European Union Agency for Network and Information Security) publishes a yearly “Annual Incident Report” for the telecommunication sector. The states’ NRAs (National Reporting Agencies) collect the incidents that are mandatory to be reported and forward them to the ENISA. This procedure is defined in the European Directive 2009/140/EC on a common regulatory framework for electronic communications networks and services, art. 13 a. Since 2011, the number of reporting member states has come up to 30 (see figure 2). Figure 3 shows the percentage of services impacted by the reported incidents. Mostly, more than one kind of service has been disturbed, so the sums are above 100 %. Figure 4 shows to what extend the emergency calls have been impacted by the incidents (also in percentage): up to 1/3 of the disruptions also affected emergency calls. Which components of the telecommunication system are most vulnerable is shown in figure 5. Switches and user and location registers are the most affected assets when a disruption occurs, which indicates that a lot of incidents have impact on a local / household basis. The assets listed in figure 5 can also be of interest for RESISTO’s use case definitions.

Reference for figures 2 to 5 is the data from the “Annual Incident Reports”, available on the ENISA website [ENI2019a].

The data shows that the European telecommunication infrastructure is vulnerable, especially the mobile services. And, as can be seen in chapter 5.3, it is especially prone to system failure regarding the number of affected users and especially prone to natural hazards, but also combined physical and cyber threats regarding the duration of disruptions.

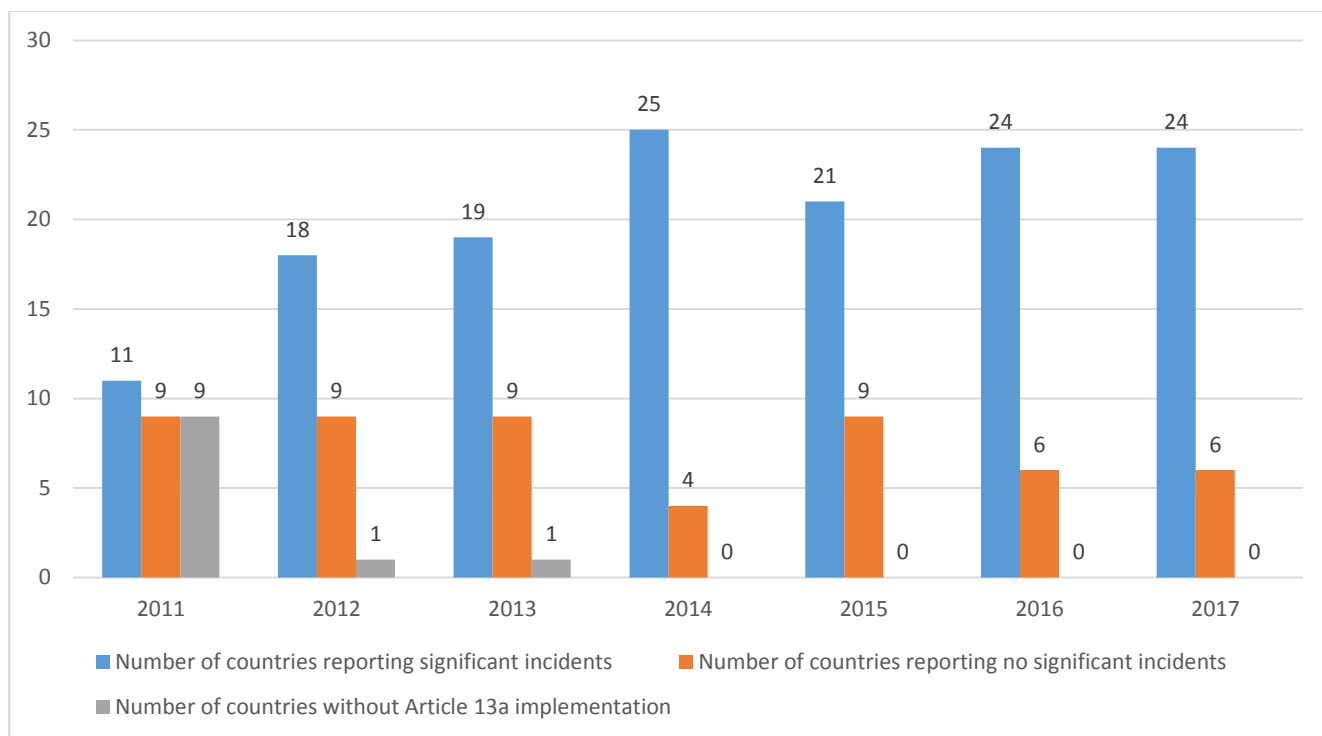


Figure 2 – Numbers of countries reporting incidents to their NRAs [ENI2019a]

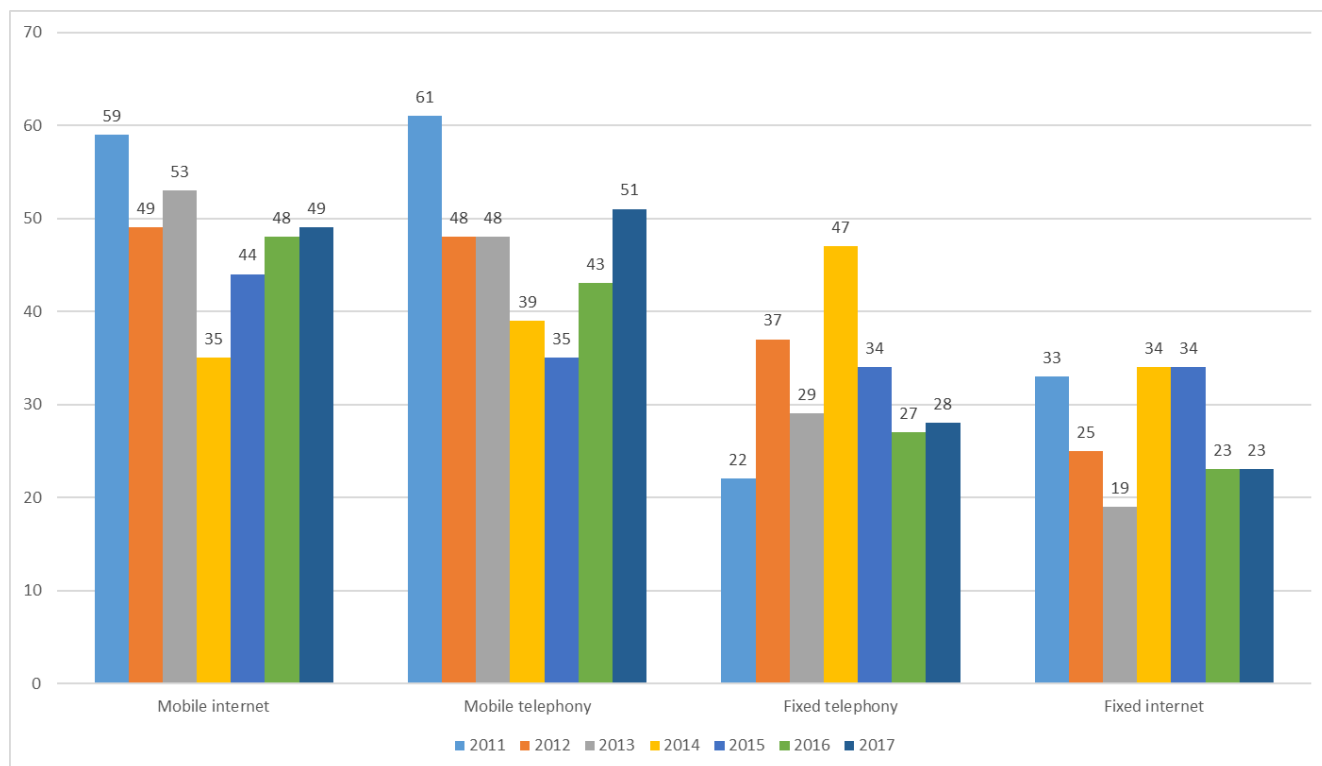


Figure 3 – Impact of incidents on classic services in percent [ENI2019a]

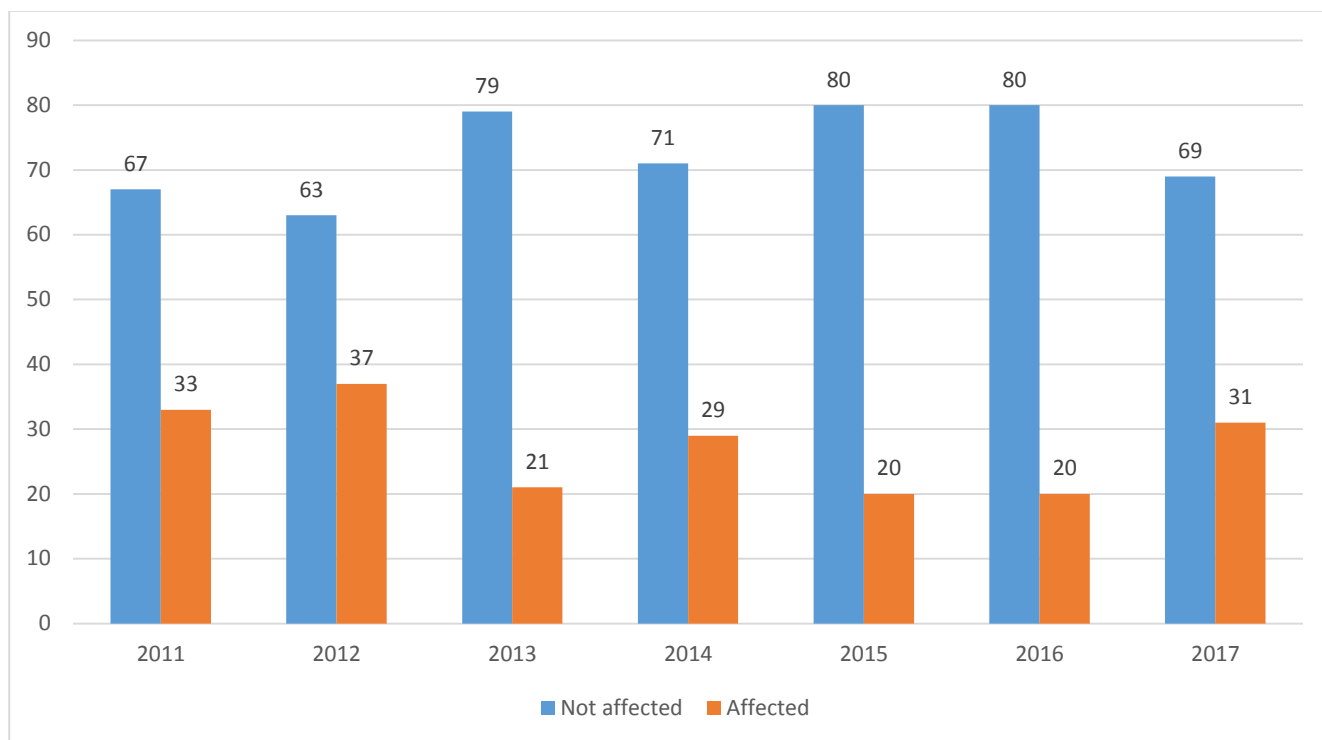


Figure 4 – Impact of incidents on emergency calls in percent [ENI2019a]

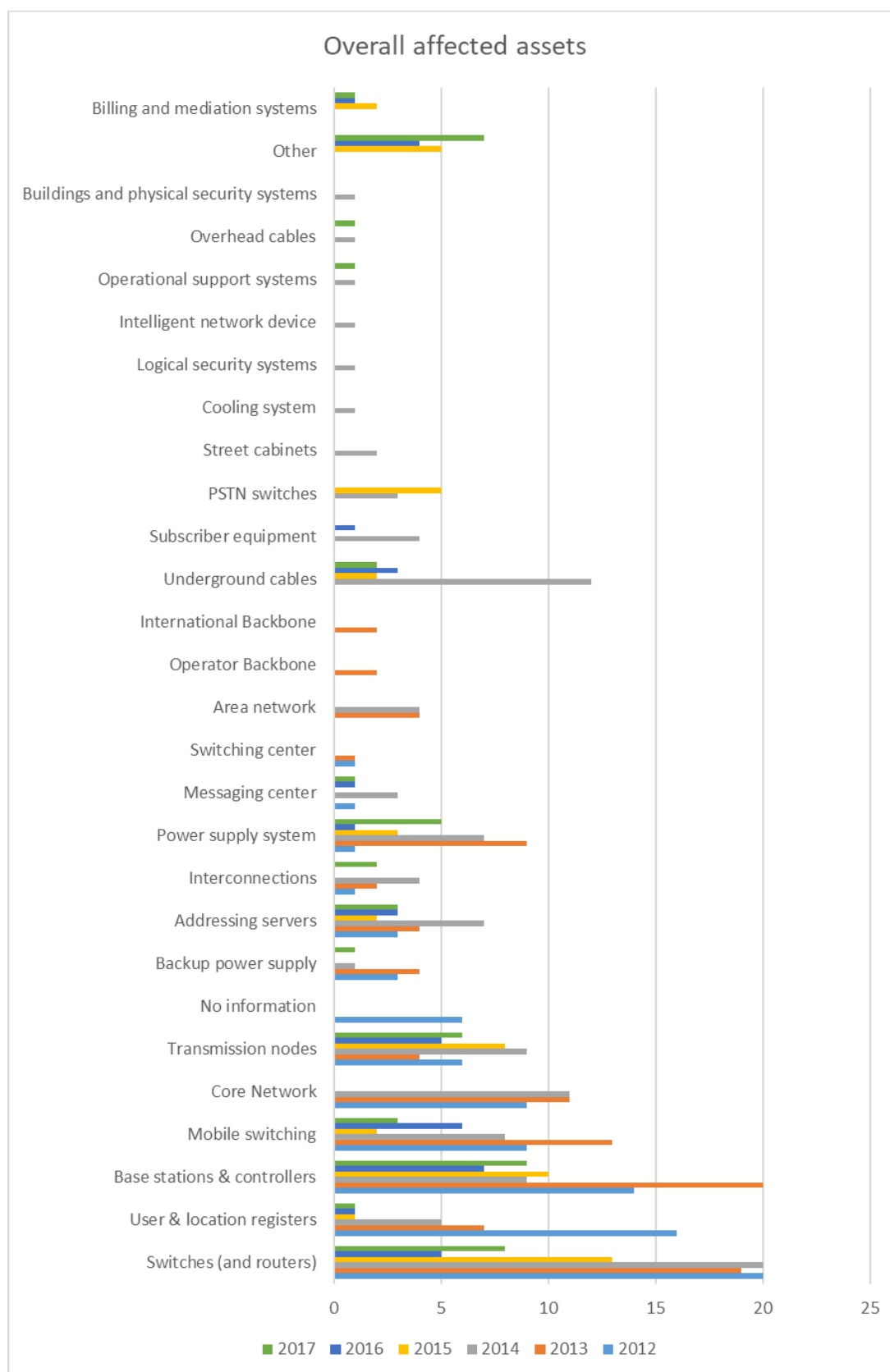


Figure 5 – Overall by incidents affected assets [ENI2019a]

As it can be derived from the above figures and the ENISA overall report [ENI2019b] (see figure 6 below), not only the telecommunication infrastructure is vulnerable, but also the vulnerabilities and threats in telecom infrastructures tend to increase from year to year. In the following, an overview of the current threat landscape and a comparison with the previous year is given.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	↻	1. Malware	↻	→
2. Web Based Attacks	↻	2. Web Based Attacks	↻	→
3. Web Application Attacks	↻	3. Web Application Attacks	↻	→
4. Phishing	↻	4. Phishing	↻	→
5. Spam	↻	5. Denial of Service	↻	↑
6. Denial of Service	↻	6. Spam	↻	↓
7. Ransomware	↻	7. Botnets	↻	↑
8. Botnets	↻	8. Data Breaches	↻	↑
9. Insider threat	↻	9. Insider Threat	↻	→
10. Physical manipulation/ damage/ theft/loss	↻	10. Physical manipulation/ damage/ theft/loss	↻	→
11. Data Breaches	↻	11. Information Leakage	↻	↑
12. Identity Theft	↻	12. Identity Theft	↻	→
13. Information Leakage	↻	13. Cryptojacking	↻	NEW
14. Exploit Kits	↻	14. Ransomware	↻	↓
15. Cyber Espionage	↻	15. Cyber Espionage	↻	→
<b>Legend:</b> Trends: ↻ Declining, ↻ Stable, ↻ Increasing Ranking: ↑ Going up, → Same, ↓ Going down				

Figure 6 – Overview and comparison of the 2018 threat landscape [ENI2019b]

From the above diagram it can be seen that new threats are inserted in the telecom infrastructures landscape, while certain of the existing threats such as information leakage or physical manipulations are the outcomes of combined cyber-physical threats in telecom CIs. One of the focuses of the RESISTO project is this combination of cyber and physical hazards. Here, not only the combination but also the sequences are of interest, for example a cyberattack producing a physical consequence such as the propagation on other CI or physical intrusions injecting cyber malware.



## 5.2 Societal impact of disruptions

The International Telecommunication Union ITU publishes statistics about the numbers of fixed and mobile telephone subscriptions in each member country. Figure 7 shows the data from 2005 to 2018.

The fact that the numbers of fixed telephone subscriptions are decreasing steadily while the number of those for mobile telephones are increasing at a significantly higher pace indicates that Europe's citizens rely heavily on being connected at all times and places. Since 2012, the mobile telephone subscriptions per 100 inhabitants exceed 120; there are 20 % more subscriptions than inhabitants.

This shows how much people rely on being accessible at any time.

As early as 1943, Maslow [MAS1943] declared security to be a basic need. Nowadays, being disconnected from family members and friends through a disruption in the telecommunication network leads to a significant reduction of the individual (and subjective) feeling of security.

The department of informatics at the University of Hamburg in Germany has listed all incidents concerning the telecommunication systems worldwide until 2013 [HIN2013]. Of special interest for them were the consequences and potential solution approaches deriving from those incidents.

Comparing the ENISA data from 2011 to 2017, there is no real trend regarding the number of affected user connections or the duration of an incident (assigned to the respective root causes system failure, human error, natural phenomenon and malicious action) (see figures 8 and 9), but with an average number of users affected of 1.429.000, system failures have the highest impact regarding spatiality. By far the longest duration of disruptions is caused by natural phenomena (55 hours in average for the years 2011 to 2017). According to the World Risk Index [BRI2016], most European countries still have a low to very low natural hazard risk. Connecting the facts that this risk is increasing and the potential effects of a natural hazard, this might be one of the most critical future challenges for telecommunication infrastructure operators.

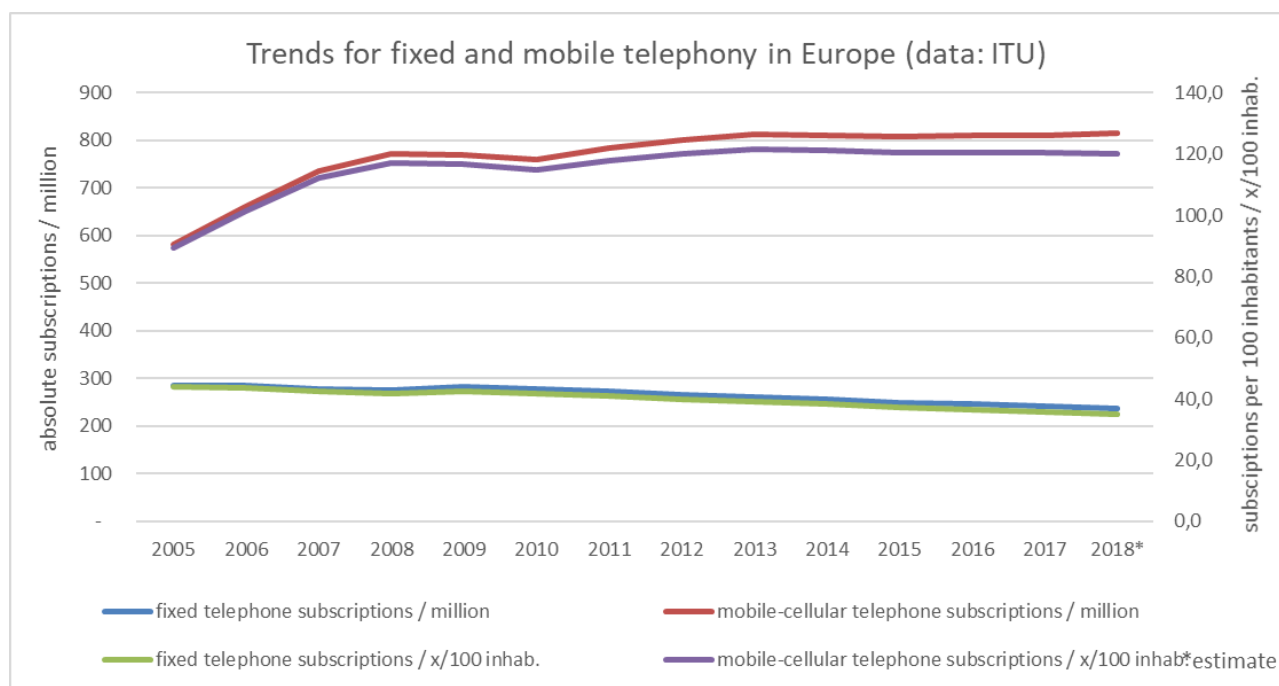


Figure 7 – Trends for fixed and mobile telephone subscriptions in Europe 2005 – 2018 [ITU2015]

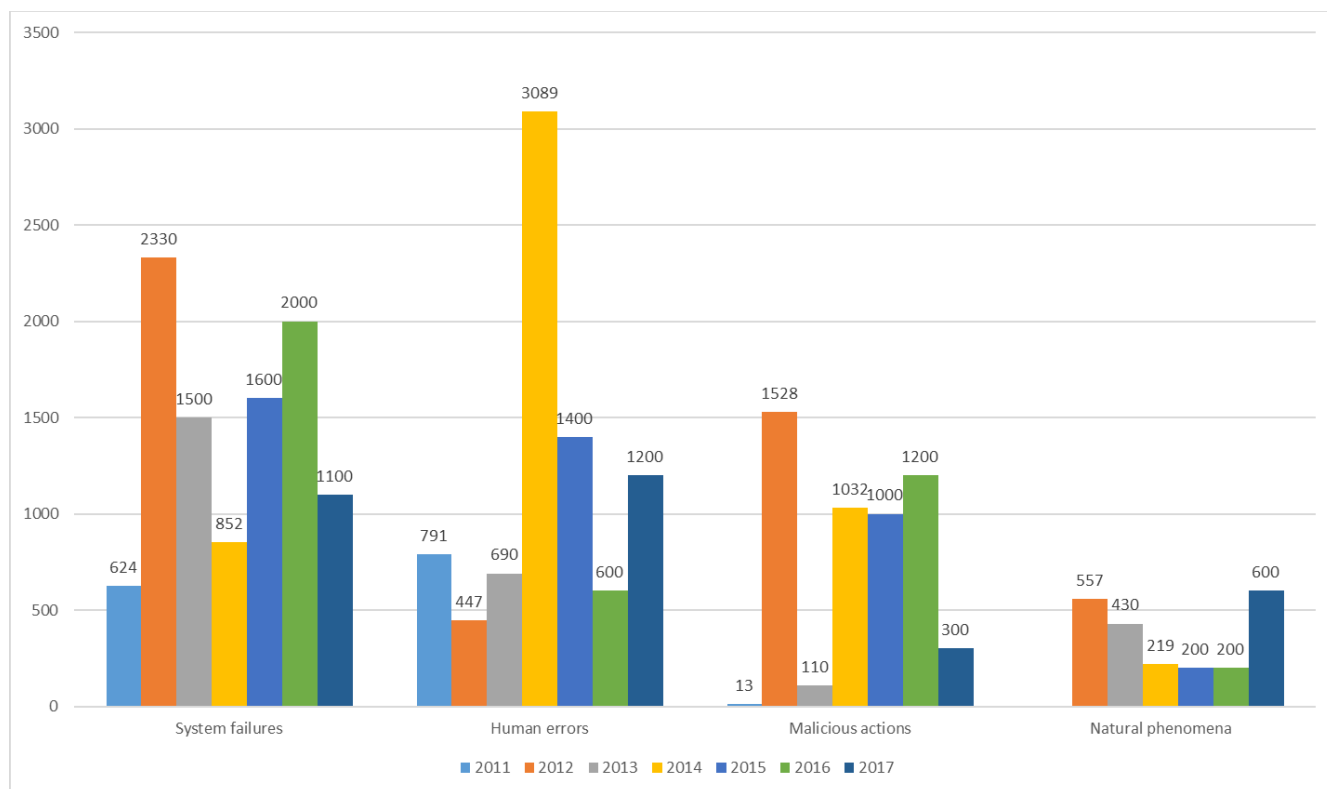


Figure 8 – Average number of user connections affected per root cause (100s), 2011 – 2017 [ENI2019a]

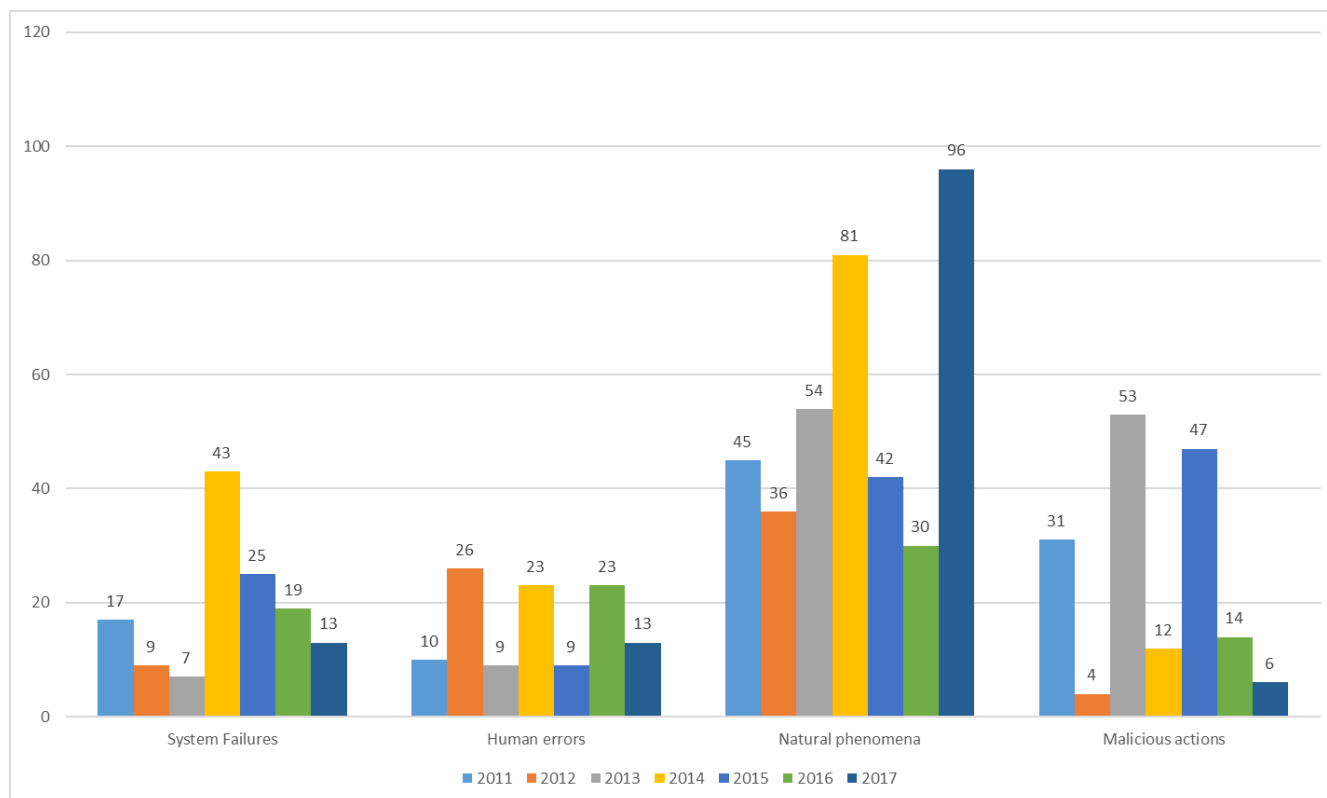


Figure 9 – Average duration of incidents per root cause (hours), 2011 – 2017 [ENI2019a]

### 5.3 Input from operators and technical experts

To collect input from operators and technical experts, a questionnaire has been designed and sent to all telco operators within the project consortium, spanning the complete telecommunication field from fiber, LTE, 5G to IoT. Five out of the six telco operating partners returned their questionnaires and this chapter evaluates the most crucial part of the answers. The whole questionnaire including the anonymized answers is shown in annex 1.

The questions are divided into chapters, following the nine steps approach for the resilience management process [HAE2018]: context analysis (5.3.1), system analysis: including environment and interface analysis, boundary definitions and (graphical) modelling (5.3.2), system performance function identification (5.3.2), disruption identification (5.3.4), pre-assessment of the criticality of system functions and disruptions (5.3.5), overall resilience quantification (5.3.6), resilience evaluation / risk acceptance / decision making (5.3.7), selection of options to improve resilience and development and implementation (5.3.8) of options improving resilience (5.3.9).

Some answers could be multiple, that is where the number of answers exceed five. Where there are less than five answers, one or more of the returns have not provided this specific information.

Not all input given here will be part of the RESISTO platform or system. It is supposed to show the state of the art of the operators / end users that are part of the RESISTO consortium and complete the picture of what is or might become important for them security-wise.

#### 5.3.1. Context Analysis

All five returns have been completed by technical staff such as engineers, stated that the respective company operates in the telecommunication industry and confirmed that they are classified as a critical infrastructure (CI). All are large enterprises with more than 250 employees. Four out of five of the responding persons are involved in the decision process regarding the implementation of security solutions, which means that the returns offer a good insight into the security structures of the companies. Three have a joint Security & Cyber Security team, in two companies those teams operate separately. IT (information technology) security is managed in-house by three, outsourced by two, physical security is managed in-house by two and outsourced by two.

A last interesting insight is, that at least three out of the five companies have agreements with other organizations such as CERT in place for exchanging potential threats information for cyber security. The other two fillers didn't know the answer to this question.

This leads to the conclusion that there's a relatively high dependency on external expert knowledge in this area, which highlights the importance of a platform like RESISTO is supposed to become.

Figures 10...14 show illustrated results of some of the questions related to context analysis.

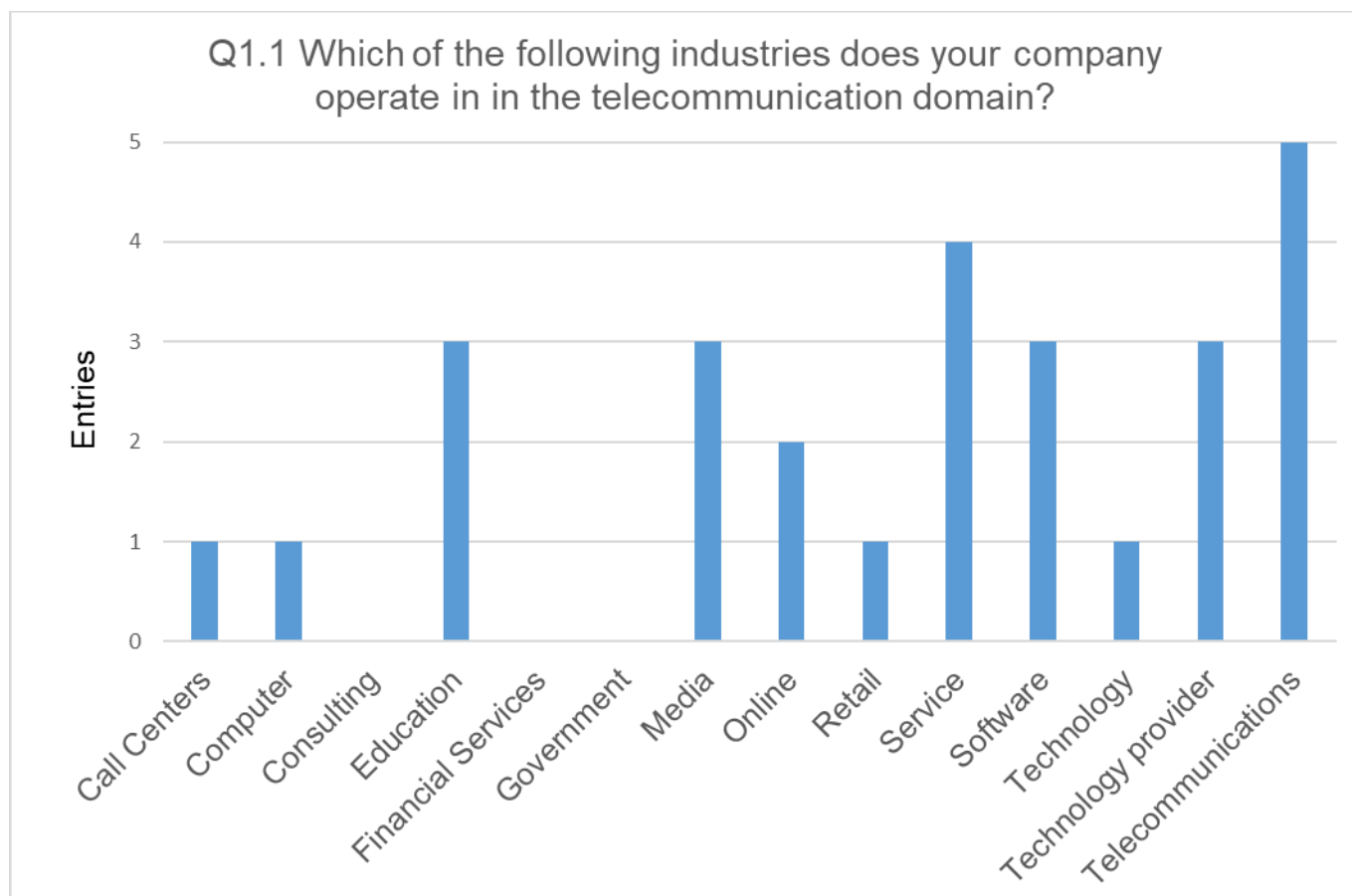


Figure 10 – Answers to Q1.1 (see annex 1) from five telecommunication operators



Figure 11 – Answers to Q1.7 (see annex 1) from five telecommunication operators

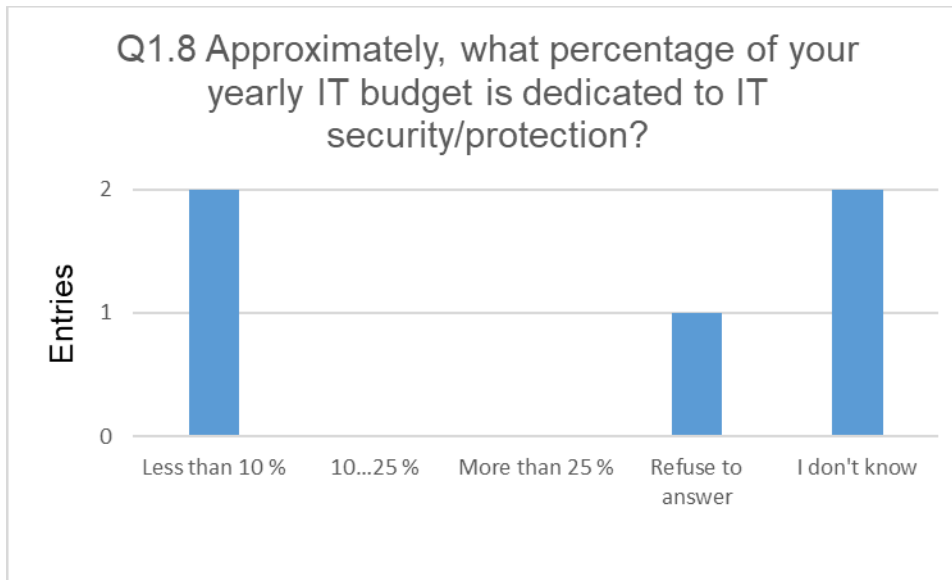


Figure 12 – Answers to Q1.8 (see annex 1) from five telecommunication operators

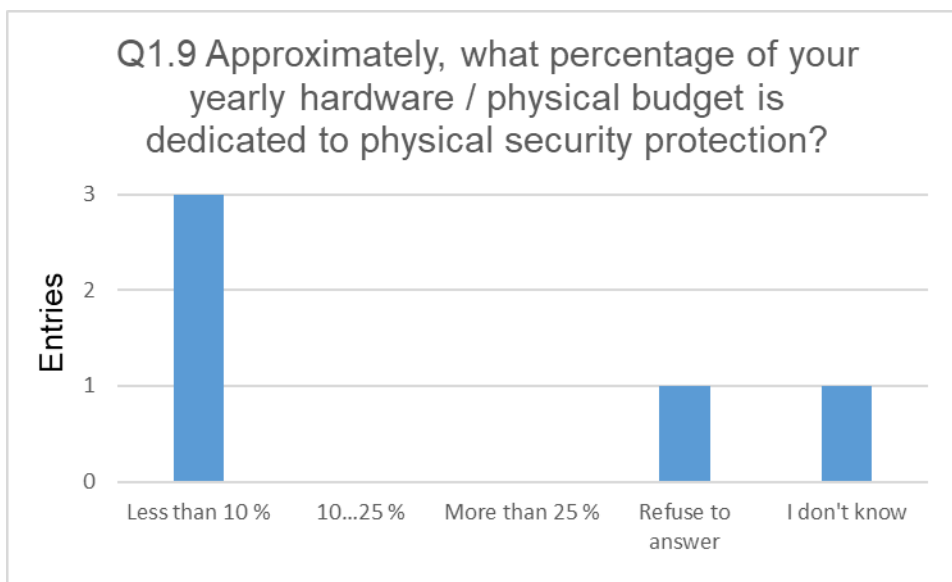


Figure 13 – Answers to Q1.9 (see annex 1) from five telecommunication operators



Figure 14 – Answers to Q1.10 (see annex 1) from five telecommunication operators

### 5.3.2. System Analysis

To be able to understand the security needs of a telecommunication operator, models of their specific system are helpful. These models offer a comprehensive insight into the system, which also means that sharing it is not lightly done. Nevertheless, one provider offered to share both their generic verbose description of their telecommunication system and a geo-referenced model of it for the development RESISTO architecture.

Three out of five consider 3...10 subsystems relevant to specify their system in terms of functionality and interconnectivity. These subsystems are not specified, except for one of the operators: Border Routers, Mobile Core, Mobile Switching Center, Radio Infrastructure, Network Security Equipment, Business Applications, Microsoft Security Domain, Servers and Workstations. Three out of those can also be found in the ENISA data (figure 5) amongst the five most frequently cited assets.

Cloud computing is handled differently, two companies use some cloud-based services, two don't use them at all, but rely fully on locally deployed datacenters. These two structures must be treated completely differently from a security point of view, which also have to be taken into account for the RESISTO platform.

In terms of interdependencies of system components, four returns state – amongst others - a function-wise reliance rather than one geographical- or hardware-wise interdependency.

The above named system models together with the requirements in chapter 6, will be a basis for the RESISTO system architecture. The alignment of requirements with affected assets during the project phase (e.g. for the use case definition) is another possible outcome.

### 5.3.3. System Performance Function Identification

One, respectively two companies provided a fully or partially completed list of (non-)performance functions that went into the requirements list (see chapter 6) and of performance functions they would like to have developed to enhance overall risk control.

Another interesting objective for RESISTO is to help the telco operators identify the relevant system components for each system function. Here, three stated a rough knowledge, one none at all and only one a detailed knowledge. This information of course is somewhere in the company's knowledge, but a wider dissemination among security related staff could be an enabler for detecting vulnerabilities and hence enhancing resilience.

#### *5.3.4. Disruption Identification*

All of those who completed the questionnaire have already experienced cyber attacks, three natural physical attacks and two man-made physical attacks. Only one experienced a cyber-physical attack.

The exposure towards the different types of risks is considered quite differently by the operators: while they consider themselves as either very exposed or exposed to cyber security attacks, the exposure towards physical attacks ranges between not exposed and very exposed. The exposure towards cyber-physical attacks is viewed as either "exposed" or "little exposed", one has not answered this question. Here, the RESISTO platform can function as an informative element to educate the operators regarding upcoming hazards that include cyber-physical attacks.

All five operators use commercial tools to detect attacks, some have additionally self-developed and/or open-source tools.

The operators agree on the sources of human-related security incidents: they either come from active employees or are classified as external attacks.

Common triggers for activating security measures are both the detection of a problem by internal tools or security equipment and the detection by a CSIRT or CERT. Two companies additionally experience user complaints as triggers.

Four out of the five operators have a communication channel for employees for incident reporting. Here, the RESISTO platform could function as an instrument for the evaluation of these reported incidents while using them to learn.

The important aspect of correlating threats, an important foreseen aspect of the RESISTO platform (coincidence, potential cascading etc.) is addressed by at least two of the companies by internal tools; two fillers didn't know about any assessment.

Figures 15 and 16 illustrate some of the questions related to disruption identification.

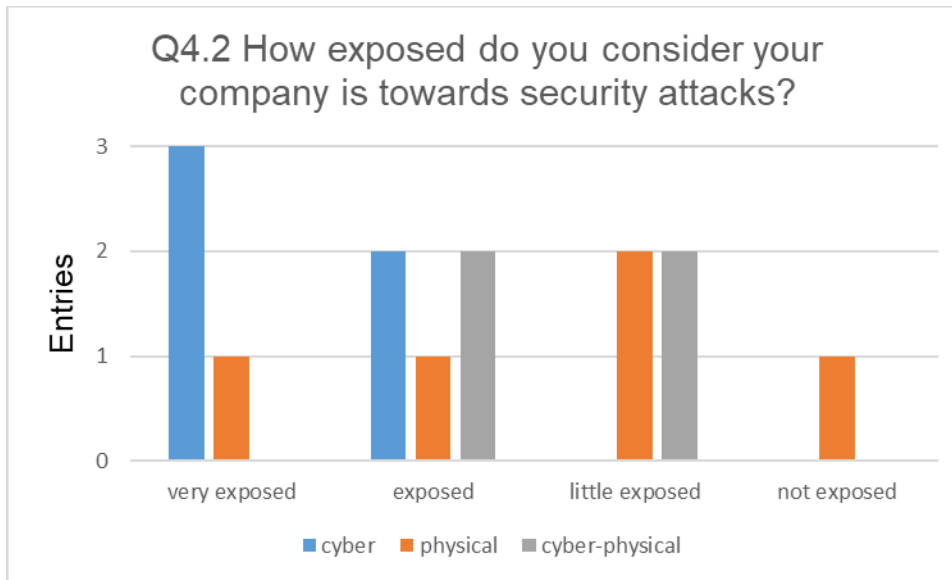


Figure 15 – Answers to Q4.2 (see annex 1) from five telecommunication operators

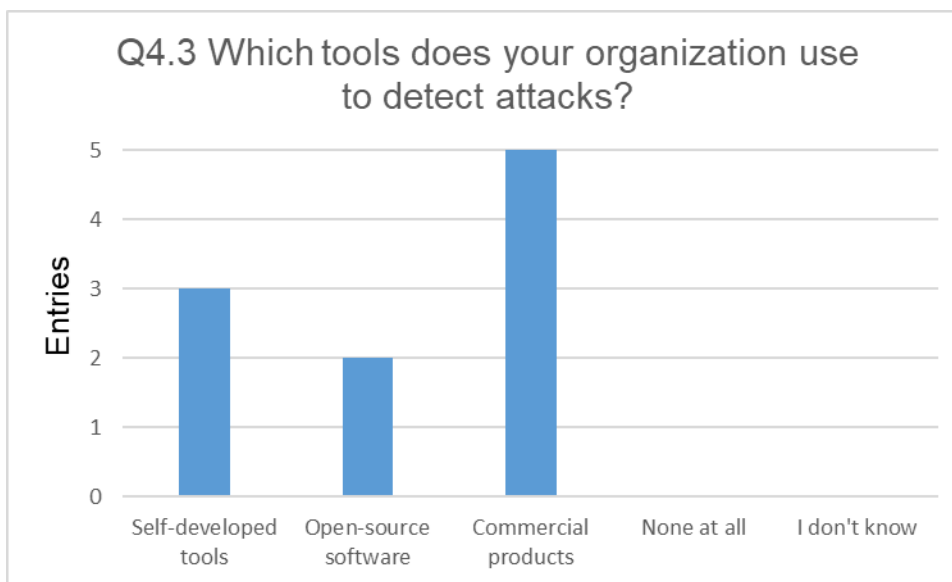


Figure 16 – Answers to Q4.3 (see annex 1) from five telecommunication operators

### 5.3.5. Pre-Assessment of the criticality of System Functions and Disruptions

The overall IT security level is rated high by all five fillers: either 8 or 9 on a scale of 10.

The level of physical security differs more, three companies rate themselves as an 8 or 9 out of 10, but two only at a 7 respectively a 5.

Four operators rely on expert rating (amongst others) when assessing the criticality of a threat – the RESISTO platform can be a useful assessment tool including a large data base.

Figures 17...19 illustrate some of the questions related to the pre-assessment of the criticality of system functions and disruptions.



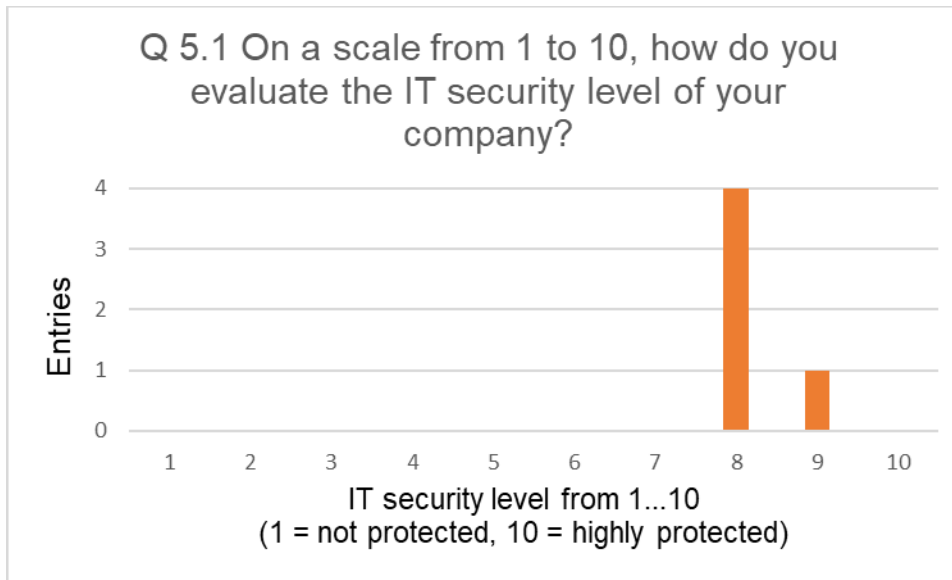


Figure 17 – Answers to Q5.1 (see annex 1) from five telecommunication operators

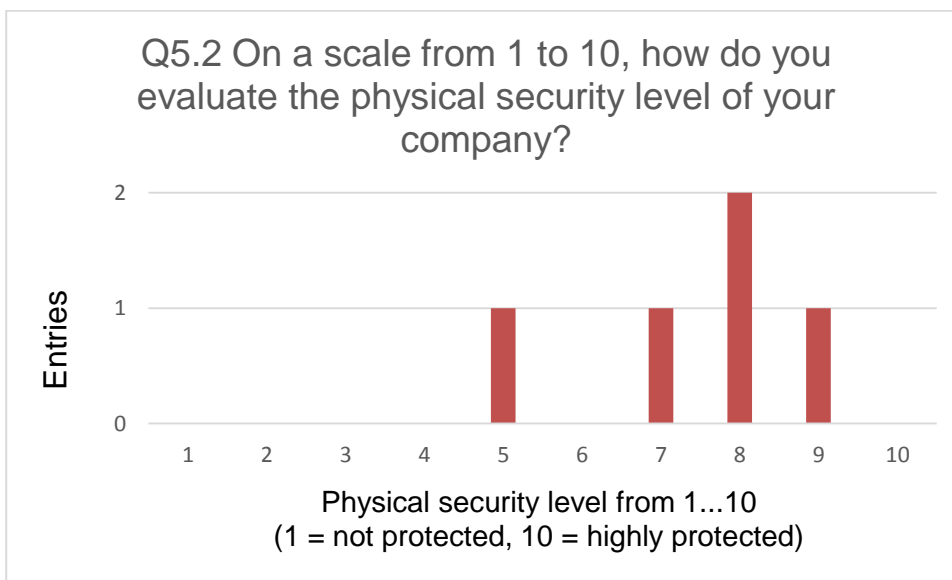


Figure 18 – Answers to Q5.2 (see annex 1) from five telecommunication operators

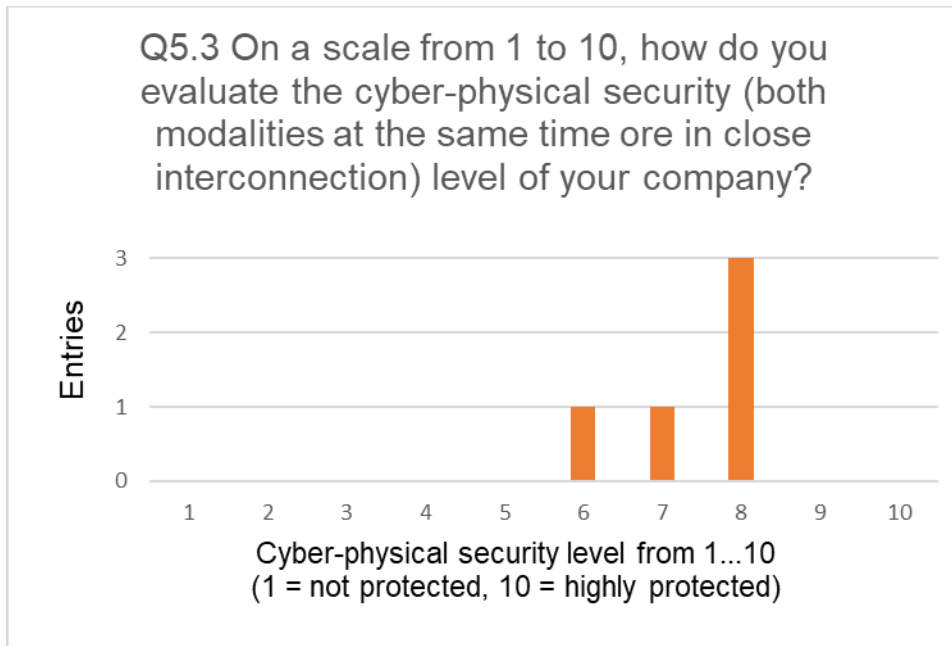


Figure 19 – Answers to Q5.3 (see annex 1) from five telecommunication operators

#### 5.3.6. Overall Resilience Quantification

Four out of five use a commercial Security Information and Event Management solution (SIEM) and three have a Security Operations Center (SOC) on-site. All conduct cyber security audits such as penetration tests.

Three of the five operators do not integrate their cyber security and physical security systems. That is an interesting fact, considering that three of the companies have a joint Security & Cyber Security team (see 5.3.1).

The RESISTO project focusses on the unified physical-cyber approach to address the upcoming issue of combined threats.

#### 5.3.7. Resilience Evaluation / Risk Acceptance / Decision Making

Four out of the five companies determine the acceptability of a risk both via economic and technology driven factors. Two also list the press/media echo as relevant and “severity” has been included by individual text.

The RESISTO system has to reflect these factors as they define the main drivers for risk evaluation.

#### 5.3.8. Selection of Options to improve Resilience Development and Implementation

Here, the fillers had the opportunity to specify their wishes regarding the RESISTO platform.

Four out of five would find information about affected components, affected system functions and the components linked to the affected system functions useful to manage hazards easier.

All would favor a graphical representation of this information, two would additionally like a tabular or text based web interface.

A risk management software is considered a useful software tool by all five fillers.

The chances and risks of relatively new or upcoming technologies such as IoT, AI, machine learning, blockchain technology or 5G have also been subject in this part of the questionnaire. Except for blockchain technology, which is overall considered as a useful asset for critical infrastructure protection, the opinions differ greatly here (see questions 8.7 to 8.10 in annex 1).

#### *5.3.9. Development and Implementation of Options improving Resilience*

Regarding existing security measures such as remote access policy, external devices on the premises or authentication mechanisms, the answers vary too much to be summarized here (please see questions 9.4 to 9.8 in annex 1).

Regarding the regular training of staff, all five companies follow routines which are not specified by this survey.

## 6. REQUIREMENTS

The following chapters list the requirements – following the systematics described in chapter 4 – the telecommunication infrastructure operators and other technical experts from the RESISTO consortium provided.

The first two subchapters (6.1 functional and 6.2 non-functional requirements) list all collected requirements, ordered only in accordance to technical classifications. Chapter 6.3 is an extraction of those requirements that were found to be mandatory, i.e. they need to be included in the system architecture of RESISTO during the project phase, where TRL 7 is the target.

The difficulty in the collection lay in the fact that the operators and experts define a specific chapter heading according to their organizational vocabulary which might differ from the vocabulary used in another company. Therefore, the final list is a comprehensive approach and the different definitions shall help RESISTO to learn to interpret the language of its end-users.

The identity codes have gaps of ten in their numbers to be able to insert new requirements whenever they occur – during the system development phase or when in use.

Most requirements are referring to the RESISTO system/platform in general. Where a specific component is addressed, it is highlighted in *italic*.

The requirement level can be **SHALL** (mandatory during project phase), **SHOULD** (recommended or highly recommended, especially if and when the RESISTO platform will be completed and run in a production environment (TRL 8 and 9)) and **COULD** (neither mandatory nor highly recommended).

The requirement verifiability can be **T** for test, **D** for demonstration, **I** for inspection or **A** for analysis. Requirements without a verification method in the list will be assigned to one during the implementation process. For each requirement the verification method mentioned here is just an indication to be confirmed or changed during the validation phase.

For further explanations regarding the classifications, see chapter 4.

For information on the system concept as well as a system preliminary architecture, see deliverable D2.6.

### 6.1 Functional Requirements

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_0005	RESISTO <b>shall</b> exploit the outcomes of the cyber security and the physical security systems of the TLC infrastructures (if existing).	D
RES_FUN_0006	RESISTO <b>shall</b> provide physical intrusion detection based on a variety of sensors, such as audio/video/radar and other passive and active sensors.	D
RES_FUN_0010	The RESISTO system <b>should</b> be able to detect Cyber/Physical threats, e.g. related to the cloud infrastructure.	D
RES_FUN_0020	Physical threats detection of the RESISTO platform <b>should</b> include data collected from sensors protecting access to systems.	D
RES_FUN_0030	The RESISTO system <b>shall</b> be able to receive, collect and process alert events relevant to physical detection.	D

RES_FUN_0040	The RESISTO system <b>should</b> be able to define maintenance windows where alarms are traced.	D
RES_FUN_0050	The RESISTO system <b>could</b> maintain a historical case of events, and could be able to correlate events.	D
RES_FUN_0060	The RESISTO system <b>should</b> collect events coming from the existing external systems of the end users (e.g. notified by the operating system and by the hardware event collector, the removal of system hardware like disks, changes in the Hardware/Software configurations)	D
RES_FUN_0070	RESISTO <b>shall</b> suggest to the operator the necessary steps to mitigate the effect of a cyber/physical attack.	D
RES_FUN_0080	In case of a security event the RESISTO system <b>should</b> be able to represent a timeline of a security event on a specific asset of platform.	D
RES_FUN_0100	The RESISTO system <b>shall</b> collect non-authorized personnel access inside the telecom facility if provided by the operator.	D
RES_FUN_0110	The RESISTO system <b>should</b> be able to help avoiding telecom facility equipment and/or private information theft by collecting data from specific sensors and providing mitigation measures.	D
RES_FUN_0130	The RESISTO platform <b>should</b> include a tool to detect radio interference, such as from Wi-Fi or cellular networks whose coverage spans the telecom facility or radio jammers.	D and/or A
RES_FUN_0200	The RESISTO system <b>should</b> detect different kinds of attacks: cyber and physical ones.	D
RES_FUN_0210	The RESISTO system <b>should</b> state the criticality of the attack.	D
RES_FUN_0220	The RESISTO system <b>should</b> inform the operator on first impact.	D
RES_FUN_0230	The RESISTO system <b>should</b> send the response and mitigation measures as a message to the operator.	D
RES_FUN_0240	The RESISTO system <b>should</b> estimate impact propagation of an attack, also to other interconnected CIs.	D
RES_FUN_0250	The RESISTO system <b>could</b> inform on estimated remaining time to solve the problem.	D
RES_FUN_0260	The RESISTO system <b>should</b> suggest actions to recover and enhance resilience.	D
RES_FUN_0270	The RESISTO system <b>should</b> have separate between the time-critical detection and prevention.	D

RES_FUN_0275	The RESISTO system <b>should</b> include audio and visual analytics functionalities.	D
--------------	--	---

#### 6.1.1. Input Data

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_0280	The RESISTO system <b>should</b> be able to receive threat and alert related data from the cloud platform or other systems.	D
RES_FUN_0290	RESISTO <b>should</b> monitor external sources such as from social media to be alerted of security threats occurring worldwide in order to prevent security threats.	D
RES_FUN_0310	If the operation requires spatial-temporal information, the input data of the RESISTO system <b>should</b> include desensitized/non-desensitized spatial-temporal data, depending on the use cases, e.g. the geo-location information of infected devices.	D
RES_FUN_0320	The input data of the RESISTO system <b>could</b> also include data sources containing the network information, e.g. the network traffic directional data, if network information are needed for the operation and response.	D
RES_FUN_0330	RESISTO <b>could</b> be able to receive new crime and incident data from Telco operators' crime and incident data stores.	D
RES_FUN_0340	RESISTO <b>could</b> be able to use appropriate data from Public data sources such as crime data from police, weather data, and utility companies such as power cuts.	D
RES_FUN_0350	RESISTO <b>could</b> be able to receive and process data from Telcos' fault management systems. These include network faults, equipment faults, and etc.	D
RES_FUN_0390	The RESISTO system <b>shall</b> have a whitelist with all authorized radio devices inside the telecom facility.	I
RES_FUN_0400	The RESISTO system <b>shall</b> have a list of all authorized cells or base stations and their operating frequency range in a target area.	I
RES_FUN_0550	The <i>Mitigation Module</i> <b>shall</b> provide automated or semi-automated mitigation responses based on pre-defined templates.	D
RES_FUN_0560	The <i>Risk (Impact) Predictor</i> <b>shall</b> also include a network impact as well.	D
RES_FUN_0570	The <i>Risk and resilience assessment analysis</i> <b>shall</b> also take into consideration network single point of failure nodes, using network metrics such as: <ul style="list-style-type: none"> <li>✓ Link state protocol databases for alternative IGP routes</li> <li>✓ BGP secondary paths for EGP routes</li> </ul> HSRP/VRRP/GLBP statuses for gateway redundancy.	D
RES_FUN_0585	The RESISTO platform <b>shall</b> provide a mitigation action	D

	at run-time when any backup resource will not be available anymore.	
--	---	--

### 6.1.2. System Work-Flows

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_0630	The RESISTO system <b>should</b> allow the provisioning of best practice workflow templates.	D
RES_FUN_0810	The <i>Risk and resilience assessment analysis</i> <b>should</b> also take into consideration traffic flows through network devices and offer upgrade suggestions in case of traffic increase based on device capabilities (throughput, processor, memory, etc.).	D
RES_FUN_0820	The <i>Map Viewer</i> <b>could</b> include a Threat Map of the suspicious traffic, based on traffic flows and IPS/IDS sensors.	D

### 6.1.3 Vulnerability Disclosure

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_0660	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to authenticate users and security researchers.	D
RES_FUN_0670	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to provide users with functionalities to define the scope for testing, rewards for different types of threats.	D
RES_FUN_0680	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to allow Security Researchers to submit findings.	D
RES_FUN_0690	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to reward Security Researchers based on a matrix of rewards defined by users.	D
RES_FUN_0700	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to help Security Researchers and users to monitor vulnerabilities reported through the whole cycle: <ul style="list-style-type: none"> <li>✓ report the finding,</li> <li>✓ confirm/reject/request additional information from the security researcher,</li> <li>✓ notify the stakeholders,</li> <li>✓ patch the finding,</li> <li>✓ confirm from the security researcher that the issue was fixed,</li> <li>✓ reward the security researcher, if appropriate.</li> </ul>	D



#### 6.1.4. System Reports and other Output

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_0845	RESISTO <b>should</b> be able to classify information or security events (for example Traffic Light Protocol - TLP).	D
RES_FUN_0850	The <i>Smart Spectrum Surveillance (SSS) tool</i> <b>should</b> periodically or on operator demand generate a report with a summary of the events that the SSS is able to detect (non-registered radio devices presence for the Access Control module and non-registered/missing cells or interferences in the Cell Monitor module).	D
RES_FUN_0870	The RESISTO platform <b>shall</b> be able to produce a report for each attack/mitigation action set containing relevant elements such as duration of the attack, types of traffic or sensors that triggered the attack for security insight, etc.	D
RES_FUN_0900	The <i>Vulnerability Disclosure Framework</i> <b>should</b> have a module called "Hall of Fame" that organises security researchers based on the total number of findings score received from the users.	D
RES_FUN_0960	The <i>Airborne Threats Detector</i> <b>should</b> have reports available in the Cockpit.	D
RES_FUN_1040	The RESISTO system <b>shall</b> support the distribution of human-readable reports in industry-standard formats such as .PDF or .HTML.	D
RES_FUN_1050	The RESISTO system <b>should</b> support the output of report data through a secure connection to a RESTFull API End-Point, in JSON format.	D

#### 6.1.5. Data Input Permission

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_FUN_1060	The RESISTO system <b>should</b> offer different levels of controls regarding who could access the raw data.	D
RES_FUN_1080	The access to RESISTO system configuration and data <b>should</b> be determined by Role Based Access Control (RBAC) policies and <b>should</b> support RBAC scheme for granular multi-user multi-role functionality.	D
RES_FUN_1100	All software modules of RESISTO <b>should</b> be checked for remote access filter compliance (access-lists applied on remote access – management interfaces).	D
RES_FUN_1105	The RESISTO platform <b>shall</b> ensure user access authentication according to the security requirements.	D
RES_FUN_1106	All users of the RESISTO platform <b>shall</b> be authenticated.	D



### 6.1.6. Functional Requirements related to 5G

Requirement Identity Code	Requirement description	Requirement Verifiability
RES_FUN_1107	The RESISTO system <b>shall</b> be able to order the seamless relocation and restoration of virtualized network resources in the event of failure or cyber/physical attack if provided by the operator control system, such that service continuity can be guaranteed.	
RES_FUN_1108	The RESISTO system <b>shall</b> maintain updated information of compute, storage and network resources within the relevant infrastructure domain.	
RES_FUN_1109	The RESISTO system <b>should</b> be able to interoperate with standard management and orchestration frameworks for virtualized network infrastructures, namely NFV MANO (resp. recommendations: ETSI GR NFV-IFA 012 and ETSI GS NFV-IFA 013).	

## 6.2 Non-Functional Requirements

### 6.2.1. Design Requirements

Requirement Identity Code	Requirement Description	Requirement Verifiability
RES_DCC_0010	The <i>Knowledge Base</i> items <b>should</b> have a standard format for the item definition, such as a json object.	D
RES_DCC_0030	The gateway layer from <i>KSI Infrastructure</i> <b>should</b> be hosted on-premise.	D
RES_DCC_0040	Some modules of the RESISTO system <b>should</b> support virtualization at the OS level for fast horizontal scaling in the Datacenter environment.	
RES_DCC_0050	The RESISTO system <b>should</b> be available for different network types.	

### 6.2.2. Implementation Requirements

Requirement Identity Code	Requirement Description	Requirement verifiability
RES_IMP_0010	The <i>Smart Spectrum Surveillance</i> <b>shall</b> provide an interface in the Cockpit in order to change settings for the composing tools.	D

### 6.2.3. Interface Requirements

Requirement Identity Code	Requirement Description	Requirement verifiability
<b>USER INTERFACES</b>		
RES_INT_0010	The user interface of the RESISTO system <b>should</b> give the operator a summary of all the events occurred on systems, with the ability to drill down a particular event to investigate and to have a historical view of similar events, and review the necessary steps taken to resolve the issue.	
RES_INT_0020	RESISTO <b>should</b> be able to represent several Dashboards, one for Real Time events, and one with historical data.	D
RES_INT_0030	The operator of the RESISTO system <b>should</b> have the ability to classify (for example from the GUI) with the use of a “tag” the security events, group of security events and their correlated assets of the platform.	
RES_INT_0040	Common user interface components of the RESISTO system <b>could</b> include summary statistics.	
RES_INT_0060	The common user interface components of the RESISTO system <b>could</b> include visual analytics by geo-location.	
RES_INT_0080	The user interfaces of the RESISTO system <b>should</b> also include the navigation functionalities to navigate through the spatial representation of the data.	
RES_INT_0090	The RESISTO system <b>should</b> include drill down information and analytics pages or views when clicking on different visualizations of data.	
RES_INT_0100	The user interfaces of the RESISTO system <b>should</b> include options for the users to set up and select different models and to visualise the prediction results.	
RES_INT_0110	The RESISTO system <b>could</b> include functionalities for the users to take any mitigation measures such as (indicatively) manage the rule engine or the ticketing system to mitigate the threats.	
RES_INT_0120	RESISTO <b>should</b> include alerts and their severities. Clicking alerts should drill down to details of the alerts, i.e. what triggered the alerts and the data behind (evidence support them).	
RES_INT_0130	The RESISTO system <b>should</b> offer a holistic view of network healthy highlighting what networks running smoothly and what networks have unresolved issues and their severities are color or shape encoded so operators could easily to see.	
RES_INT_0140	The RESISTO system <b>should</b> be links seamlessly allow operators to create jobs to deal with alerts.	
<b>SOFTWARE INTERFACES</b>		
RES_INT_0190	RESISTO platform <b>should</b> be able to control operators network equipment supporting standard API (json or XML based preferred ) calls.	D
RES_INT_0220	Each user <b>should</b> have one API access key per each	D

	dataset the user is permitted to have access to.	
<b>COMMUNICATION INTERFACES</b>		
RES_INT_0230	Network interfaces of the Virtual Machines that host RESISTO components <b>shall</b> offer full support for both IPv6 and IPv4 TCP stacks.	D
RES_INT_0240	Network interfaces <b>shall</b> support standardized IEEE 802.3 Ethernet technology for interoperability.	D
RES_INT_0250	Network elements inside the platform <b>should</b> reserve bandwidth for marked network traffic (interface feature).	D

#### 6.2.4. Security Requirements

Requirement Identity Code	Requirement Description	Requirement verifiability
<b>GENERAL</b>		
RES_SEC_0010	RESISTO <b>should</b> ensure that users and applications are identified and that their identities are properly verified.	D
RES_SEC_0020	RESISTO <b>should</b> ensure that users and applications can only access data and services for which they have been properly authorized.	D
RES_SEC_0030	RESISTO <b>should</b> detect attempted intrusions by unauthorized persons and applications.	D
RES_SEC_0040	RESISTO <b>should</b> enable security personnel to audit the status and usage of the security mechanisms.	D
RES_SEC_0050	RESISTO <b>should</b> ensure that unauthorized malicious programs do not infect the application or components.	D
RES_SEC_0060	RESISTO <b>should</b> ensure that communications and data are not intentionally corrupted.	D
RES_SEC_0070	RESISTO <b>should</b> ensure that confidential communications are kept private.	D
RES_SEC_0080	RESISTO <b>should</b> ensure that all components survive attacks.	D
RES_SEC_0090	RESISTO <b>should</b> ensure that systems (both people and application) are protected against destruction, damage, theft).	D
RES_SEC_0100	The RESISTO platform <b>should</b> comply to the operator's security policies and accreditations.	D
RES_SEC_0105	The integrity of the relevant information sent by the security sensors in the system <b>shall</b> be protected by the RESISTO system.	A
<b>ACCESS CONTROL (GENERAL)</b>		
RES_SEC_0106	Each component <b>should</b> be accessible from Cockpit only after users authenticated.	D
RES_SEC_0110	Access to the RESISTO system <b>shall</b> be granted using the principle of "Least Privilege", meaning that any program, any interface, any debugging and testing	D

	console and every user of RESISTO should operate using the least set of privileges necessary to complete the job.	
RES_SEC_0120	Each user <b>shall</b> be identified by a unique user identity so that users can be linked to and take responsibility for their actions.	D
RES_SEC_0130	The use of group identities (such as Training Account, Service Accounts) <b>should</b> be permitted where they are suitable for the work carried out.	D
RES_SEC_0140	During the onboarding process to the system, each user <b>should</b> be given a copy of guidelines for staff on use of the system and their user login details and should be required to accept and confirm that they understand the conditions of access.	D
RES_SEC_0150	Records and logs of user access <b>should</b> be used to provide evidence in incident investigation and resolution.	D
RES_SEC_0160	RESISTO <b>shall</b> support the User's user access / segregation of duty requirements i.e. it supports set up of standard and group profiles.	D
RES_SEC_0170	User rights <b>should</b> be granted at the following levels: group profiles, user profiles, per function, per field within a function.	D
RES_SEC_0180	Rights to all component data and objects <b>should</b> be delegated to a user profile, not a user.	D
RES_SEC_0190	User profiles <b>should</b> have the capability of restricting access to data, this being either: Full read/write access, Read only access, No Access.	D
RES_SEC_0200	The platform <b>should</b> support simultaneous multiple user logons.	D
RES_SEC_0210	The input into platform <b>should</b> be validated before further processing to prevent the injection of malicious code.	D
RES_SEC_0220	User <b>should not</b> be able to break-out of the application to obtain command line access to the application server.	D
RES_SEC_0230	If web applications will be part of Resisto, Implement anti-browser caching and Cookies <b>should not</b> include sensitive data, specifically authentication or any other security that may lead to the compromise of the application.	D
RES_SEC_0240	An Information Classification on all data produced by the RESISTO platform <b>should</b> be provided. For example, Strictly Confidential, Confidential, Restricted etc.	D
RES_SEC_0245	Platform <b>shall</b> support remote login using encrypted protocols, such as HTTPS and SSH with only TLSv1.2 or above algorithms.	D
<b>ACCESS CONTROL (NETWORK ACCESS)</b>		
RES_SEC_0250	Access rights to the RESISTO platform resources (services, functions, data, etc.) <b>should</b> be regulated based on the attributes or roles of the authenticated end users, according to the general access control requirements.	T

RES_SEC_0260	Policies expressed in standard policy language such as XACML <b>could</b> be used to support the access control mechanism.	T
RES_SEC_0270	All staff and third parties <b>should</b> be given access to the RESISTO network in accordance with business access control procedures and requirements for access defined by their roles	D
RES_SEC_0280	All staff and third parties who access the RESISTO network remotely <b>shall</b> only be authenticated using the approved remote access authentication mechanism	D
RES_SEC_0290	Diagnostics and configuration ports <b>should</b> only be enabled for specific business reasons. Communication on all other ports <b>should</b> be disabled	D
RES_SEC_0300	The network access to the Resisto platform <b>should</b> be protected with encryption of the communication.	D
RES_SEC_0310	The network access to the Resisto platform <b>should</b> be possible to grant access only from specific networks.	D
<b>ACCESS CONTROL (OPERATING ENVIRONMENT ACCESS)</b>		
RES_SEC_0320	Development environment, testing environment and operating environment for RESISTO <b>should</b> be separated.	
RES_SEC_0330	All users of the RESISTO platform will authenticate by logging in all and any components and / or interface they are required to access. A single sign-on solution and software <b>could</b> be considered for integration with all components and operating systems.	D
RES_SEC_0340	All web-based applications access <b>should</b> be secured with client certificates issued for individual users of RESISTO to install on their devices.	
<b>AUTHENTICATION</b>		
RES_SEC_0370	RESISTO <b>should</b> NOT allow login of sensitive accounts (such as those used by the applications, services and Operating Systems as back-end / middleware / databases) to any front-end user interface.	D
RES_SEC_0380	All users of the RESISTO platform <b>should</b> adhere to the Password Complexity Policy when generating a new password or changing / updating an existing password.	D
RES_SEC_0400	The password change mechanism <b>should</b> require a password length of at least 10 characters and at most 128 characters with no more than two identical characters in a row (such as 111)	D
RES_SEC_0410	The password change mechanism <b>should</b> implement a minimum topology evaluation for the old and new passwords and shall require the user to change topologies between old and new passwords	D
RES_SEC_0420	RESISTO <b>should</b> implement a secure password recovery mechanism, based on at least two factors of identification such as a required, validated e-mail address and a alphanumeric verification string sent to that address	D
RES_SEC_0430	The RESISTO platform <b>should</b> store passwords in a	D



	secure fashion, using cryptographic techniques such as -Generating of a unique salt upon creation of each stored credential -Using of cryptographically strong random data (entropy); -Using either a 32-byte or a 64-byte salt size -Scheme security does not depend on hiding, splitting or otherwise obscuring the salt	
RES_SEC_0435	RESISTO <b>shall</b> use services for protecting integrity and confidentiality of the data	D
RES_SEC_0440	The RESISTO platform <b>shall</b> transmit all passwords over a secure connection.	D
RES_SEC_0500	Option to force the user to change their password on their 1 <sup>st</sup> logon <b>should</b> be available.	D
RES_SEC_0530	The end users <b>should</b> be able to use the same user credentials to authenticate to various platform's services and tools (if applicable).	T
RES_SEC_0550	The RESISTO platform <b>should</b> implement 2FA mechanisms.	D
RES_SEC_0560	The RESISTO platform <b>should</b> integrate with external LDAP/AD systems for user SSO.	D
<b>DATA PROTECTION AND DATA MANAGEMENT (ACCESS MANAGEMENT)</b>		
RES_SEC_0580	The RESISTO Platform <b>should</b> be available for integration with existing User Access Management solutions such as MSAD, LDAP.	D
RES_SEC_0590	Authentication credentials (user-id and password) between the application client and the application server <b>should</b> be encrypted, using a strong encryption algorithm.	D
RES_SEC_0620	Sensitive data <b>should</b> be encrypted when transferred between systems.	D
RES_SEC_0625	The RESISTO system <b>should</b> use sFTP and/or SCP for file transfers – FTP <b>should</b> not be permitted.	D
RES_SEC_0640	Access to Confidential, Personal and security data <b>shall</b> be logged.	D
<b>DATA PROTECTION AND DATA MANAGEMENT (DATA IMPORT AND EXPORT)</b>		
RES_SEC_0650	RESISTO <b>shall</b> provide the user with the ability to import and export data from other systems in standard formats such as CSV, XML, XLS (e.g. "physical security alerts of a selected time interval").	D
<b>DATA PROTECTION AND DATA MANAGEMENT (DATA VALIDATION)</b>		
RES_SEC_0670	Input validation <b>should</b> be applied on both syntactical and semantic level. Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol) while semantic validation should enforce correctness of their values in the specific context.	D
<b>DATA PROTECTION AND DATA MANAGEMENT (DATA RETENTION)</b>		
RES_SEC_0690	RESISTO <b>should</b> provide the ability to store and maintain records of data that originated in RESISTO platform, was the result of input, data collection from other sources, was imported or exported from and to other systems or was generated as a result of the	D

	processing of any and all data.	
RES_SEC_0700	The RESISTO platform <b>should</b> provide the ability to retain all and any data according to a Retention Policy.	D
<b>DATA PROTECTION AND DATA MANAGEMENT (DATA PROTECTION)</b>		
RES_SEC_0720	User and system data <b>shall</b> be stored in a data store with adequate access control measures/policies complying with the GDPR.	T
RES_SEC_0730	Direct access to the platform's data store <b>shall</b> only be allowed to users with privileged access rights (such as system administrators).	T
RES_SEC_0740	Any sensitive personal user data <b>should</b> be stored in encrypted form.	T
RES_SEC_0741	The traffic between platform modules, in case of distribution across a network, <b>should</b> be encrypted using IPSec and MACSEC suite of protocols, using high-end encryptions such as AES256 and SHA256 hashing for sensitive data protection.	D
RES_SEC_0742	The <i>Repository</i> data <b>should</b> be stored encrypted in a trusted datacenter.	D
RES_SEC_0743	<i>Smart Spectrum Surveillance</i> component <b>should</b> be independently tested by security specialists, in order to confirm they are not introducing other vector of attacks in the network.	D
RES_SEC_0744	The <i>Airborne Threats Detector</i> component <b>should</b> be independently tested by security specialists, in order to confirm they are not introducing other vector of attacks in the network.	D
RES_SEC_0745	The <i>IoT Sensors</i> component <b>should</b> independently tested by security specialists in order to confirm they are not introducing other vector of attacks in the network.	D
<b>OPERATIONAL REQUIREMENTS RELATED TO SECURITY</b>		
RES_SEC_0760	The access control mechanism (i.e. authentication and authorization) of the RESISTO system <b>should</b> not introduce significant delays for accessing and using the platform services.	T
RES_SEC_0770	The management of end users of the RESISTO platform (i.e. their credentials, attributes, roles, etc.) <b>should</b> be supported by a graphical user interface.	D
RES_SEC_0790	The device and the path or IP address that any user has used to access the application <b>should</b> be logged.	D
RES_SEC_0800	All unauthorized activity (unauthorized attempts to access the application or where the user attempts to access functions for which they are not permitted) <b>should</b> be detected.	D
RES_SEC_0810	The insertion of new and update of existing database records <b>should</b> be time-stamped.	D
RES_SEC_0820	All system administrator activity <b>should</b> be logged.	D
RES_SEC_0830	Facility to filter logs based on any combination of: User-id, Command/Action performed, Date/time, Means of access <b>could</b> be provided.	D
RES_SEC_0850	Audit logs <b>should</b> be archived on a regular basis.	D

RES_SEC_0860	The platform administrator <b>could</b> be able to define what data to archive.	D
--------------	---	---

### 6.2.5. Operating Requirements

Requirement Identity Code	Requirement Description	Requirement verifiability
<b>RECOVERABILITY</b>		
RES_OPR_0125	The system <b>shall</b> be able to run on OSs and/or Virtualization environments offering “snapshot” mechanism in order to provide immediate reverse in case of major fault.	D
<b>AVAILABILITY</b>		
RES_OPR_0130	The platform <b>should</b> have a flexible architecture from the availability point of view. Based on the business needs of the operators and on the recoverability requirements, different configurations should be available to choose from: <ul style="list-style-type: none"> <li>✓ Cold-Standby</li> <li>✓ Hot-standby</li> <li>✓ Active-active</li> </ul>	D
RES_OPR_0140	All modules <b>should</b> support integration with platforms such as GIT for last-minute centralized script version controlling.	D
RES_OPR_0150	The RESISTO system <b>should</b> enable high availability of services.	

### 6.3 Mandatory Requirements

Requirement Identity Code	Requirement Description	Requirement verifiability
RES_FUN_0005	RESISTO <b>shall</b> exploit the outcomes of the cyber security and the physical security systems of the TLC infrastructures (if existing).	
RES_FUN_0006	RESISTO <b>shall</b> provide physical intrusion detection based on a variety of sensors, such as audio/video/radar and other passive and active sensors.	D
RES_FUN_0030	The RESISTO system <b>shall</b> be able to receive, collect and process alert events relevant to physical detection.	D
RES_FUN_0070	RESISTO <b>shall</b> suggest to the operator the necessary steps to mitigate the effect of a cyber/physical attack.	D
RES_FUN_0100	The RESISTO system <b>shall</b> collect non-authorized personnel access inside the telecom facility if provided by the operator.	D
RES_FUN_0390	The RESISTO system <b>shall</b> have a whitelist with all authorized radio devices inside the telecom facility.	I
RES_FUN_0400	The RESISTO system <b>shall</b> have a list of all authorized cells or base stations and their operating frequency range in a target area.	I



RES_FUN_0550	The <i>Mitigation Module</i> <b>shall</b> provide automated or semi-automated mitigation responses based on pre-defined templates.	D
RES_FUN_0560	The <i>Risk (Impact) Predictor</i> <b>shall</b> also include a network impact as well.	D
RES_FUN_0570	The <i>Risk and resilience assessment analysis</i> <b>shall</b> also take into consideration network single point of failure nodes, using network metrics such as: <ul style="list-style-type: none"> <li>✓ Link state protocol databases for alternative IGP routes</li> <li>✓ BGP secondary paths for EGP routes</li> </ul> HSRP/VRRP/GLBP statuses for gateway redundancy.	D
RES_FUN_0585	The RESISTO platform <b>shall</b> provide a mitigation action at run-time when any backup resource will not be available anymore.	D
RES_FUN_0660	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to authenticate users and security researchers.	D
RES_FUN_0670	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to provide users with functionalities to define the scope for testing, rewards for different types of threats.	D
RES_FUN_0680	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to allow Security Researchers to submit findings.	D
RES_FUN_0690	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to reward Security Researchers based on a matrix of rewards defined by users.	D
RES_FUN_0700	The <i>Vulnerability Disclosure Framework</i> <b>shall</b> be able to help Security Researchers and users to monitor vulnerabilities reported through the whole cycle: <ul style="list-style-type: none"> <li>✓ report the finding,</li> <li>✓ confirm/reject/request additional information from the security researcher,</li> <li>✓ notify the stakeholders,</li> <li>✓ patch the finding,</li> <li>✓ confirm from the security researcher that the issue was fixed,</li> </ul> reward the security researcher, if appropriate.	D
RES_FUN_0870	The RESISTO platform <b>shall</b> be able to produce a report for each attack/mitigation action set containing relevant elements such as duration of the attack, types of traffic or sensors that triggered the attack for security insight, etc.	D
RES_FUN_1040	The RESISTO system <b>shall</b> support the distribution of human-readable reports in industry-standard formats such as .PDF or .HTML.	D
RES_FUN_1105	The RESISTO platform <b>shall</b> ensure user access authentication acc. to the security requirements.	D
RES_FUN_1106	All users of the RESISTO platform <b>shall</b> be authenticated.	D
RES_FUN_1107	The RESISTO system <b>shall</b> be able to order the seamless relocation and restoration of virtualized network resources in the event of failure or cyber/physical attack if provided by the operator control	

	system, such that service continuity can be guaranteed.	
RES_FUN_1108	The RESISTO system <b>shall</b> maintain updated information of compute, storage and network resources within the relevant infrastructure domain.	
RES_IMP_0010	The <i>Smart Spectrum Surveillance</i> <b>shall</b> provide an interface in the Cockpit in order to change settings for the tools developed.	D
RES_INT_0230	Network interfaces of the Virtual Machines that host RESISTO components <b>shall</b> offer full support for both IPv6 and IPv4 TCP stacks.	D
RES_INT_0240	Network interfaces <b>shall</b> support standardized IEEE 802.3 Ethernet technology for interoperability.	D
RES_SEC_0105	The integrity of the relevant information sent by the security sensors in the system <b>shall</b> be protected by the RESISTO system.	A
RES_SEC_0110	Access to the RESISTO system <b>shall</b> be granted using the principle of “Least Privilege”, meaning that any program, any interface, any debugging and testing console and every user of RESISTO should operate using the least set of privileges necessary to complete the job.	D
RES_SEC_0120	Each user <b>shall</b> be identified by a unique user identity so that users can be linked to and take responsibility for their actions.	D
RES_SEC_0160	RESISTO <b>shall</b> support the User's user access / segregation of duty requirements i.e. it supports set up of standard and group profiles.	D
RES_SEC_0245	Platform <b>shall</b> support remote login using encrypted protocols, such as HTTPS and SSH with only TLSv1.2 or above algorithms.	D
RES_SEC_0280	All staff and third parties who access the RESISTO network remotely <b>shall</b> only be authenticated using the approved remote access authentication mechanism	D
RES_SEC_0435	Resisto <b>shall</b> use services for protecting integrity and confidentiality of the data	D
RES_SEC_0440	The RESISTO platform <b>shall</b> transmit all passwords over a secure connection.	D
RES_SEC_0640	Access to Confidential, Personal and security data <b>shall</b> be logged.	D
RES_SEC_0650	RESISTO <b>shall</b> provide the user with the ability to import and export data from other systems in standard formats such as CSV, XML, XLS (e.g. “physical security alerts of a selected time interval”).	D
RES_SEC_0720	User and system data <b>shall</b> be stored in a data store with adequate access control measures/policies complying with the GDPR.	T
RES_SEC_0730	Direct access to the platform's data store <b>shall</b> only be allowed to users with privileged access rights (such as system administrators).	T
RES_OPR_0125	The system <b>shall</b> be able to run on OSs and/or Virtualization environments offering “snapshot”	D

	mechanism in order to provide immediate reverse in case of major fault.	
--	---	--

## 7. REFERENCES

INDEX	REFERENCE
[BER2018]	Berke, P.R., Quiring, S.M., Olivera, F., Horney, J., <i>Addressing challenges to building resilience through interdisciplinary research and engagement</i> , Risk Analysis, Wiley, 2018
[BKA2010]	Bundeslagebild Cybercrime 2010 ( <a href="https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html">https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html</a> )
[BKA2017]	Bundeslagebild Cybercrime 2017 ( <a href="https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html">https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html</a> )
[BRI2016]	<a href="http://www.uni-stuttgart.de/ireus/Internationales/WorldRiskIndex/#tabs-3">http://www.uni-stuttgart.de/ireus/Internationales/WorldRiskIndex/#tabs-3</a>
[ENI2019a]	View all Annual Incident Reports here : <a href="https://www.enisa.europa.eu/topics/incident-reporting?tab=publications">https://www.enisa.europa.eu/topics/incident-reporting?tab=publications</a>
[ENI2019b]	ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends” – Final Version, 1.0, ETL2018, January 2019 Report
[HAE201]	I. Häring, Giovanni Sansavini, E. Bellini, N. Martyn, T. Kovalenko, M. Kitsak, G. Vogelbacher, K. Ross, U. Bergerhausen, K. Barker, I. Linkov, <i>Towards a generic resilience management, quantification and development process: general definitions, requirements, methods, techniques and measures, and case studies</i> , In: Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, Eds.: I. Linkov, J. M. Palma-Oliveira, Springer, Berlin, 2017
[HIN2013]	<a href="https://www.informatik.uni-hamburg.de/TKRN/world/staff/kdh/tools/netzausfaelle/netzausfaelle.html">https://www.informatik.uni-hamburg.de/TKRN/world/staff/kdh/tools/netzausfaelle/netzausfaelle.html</a>
[ITU2015]	Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications, ITU-T, 2015
[MAS1943]	Maslow, A.H., <i>A Theory of Human Motivation</i> , Psychological Review, 50 (4), 370-96, American Psychological Association, Princeton, 1943
[NRC2014]	National Research Council, <i>Reducing coastal risks on the East and Gulf coast</i> , National Academies Press, Washington, DC, 2014
[RES2018]	RESISTO – Grant Agreement. Project Starting Date: May, 1 <sup>st</sup> 2018

## ANNEX 1

<b>Questionnaire for Hazard and Disruption List / Requirements / System Performance / Security Status Quo</b>	
<b>Q1.1 Which of the following industries does your company operate in in the telecommunication domain?</b>	
Call Centers	1
Computer	1
Consulting	
Education	3
Financial Services	
Government	
Media	3
Online	2
Retail	1
Service	4
Software	3
Technology	1
Technology provider	3
Telecommunications	5
Others (please specify)	
<b>Q1.2 Is your company classified as a critical infrastructure (CI) operator?</b>	
Yes	5
No	
I don't know	
<b>Q1.3 How many employees does your company have?</b>	
<10	
10-50	
50-250	
250-2500	1
Over 2500	2
Specify the number	50000
	20305
<b>Q1.4 How many point of presence (branches, settlements) does your company have?</b>	
1-10	
10-100	
1000 - 10000	2
Over 10000	3
Specify the number	

<b>Q1.5 What is your position within the company?</b>	
IT director / IT manager	
Network administrator	
Chairman / owner	
Chief Security Officer	
Chief Information Officer	
Chief Strategy Officer	
Administrative manager	
Engineer	3
Other (please specify)	RESISTO TEAM (technology and security experts)
	Cloud Architect
<b>Q1.6 How would you describe your role regarding the implementation of security solutions?</b>	
Contribute to the decision	4
Make the final choice	
Not involved	1
<b>Q1.7 Does your company have a dedicated Security and/or Cyber Security team?</b>	
Yes, there is a joint Security & Cyber Security team	3
Yes, there are different Security & Cyber Security teams	2
No	
I don't know	
<b>Q1.8 Approximately, what percentage of your yearly IT budget is dedicated to IT security/protection?</b>	
Less than 10%	2
10%-25%	
More than 25%	
Refuse to answer	1
I don't know	2
<b>Q1.9 Approximately, what percentage of your yearly hardware / physical budget is dedicated to physical security protection?</b>	
Less than 10%	3
10%-25%	
More than 25%	

Refuse to answer	1
I don't know	1
<b>Q1.10 Do you manage your company IT Security in-house or do you outsource it to a third party?</b>	
We manage the IT Security in house	3
We outsource some security services to a MSSP (Managed Security Services Provider)	2
We outsource most security services to a MSSP	
I don't know	
<b>Q1.11 Do you manage your company physical Security in-house or do you outsource it to a third party?</b>	
We manage the physical security in-house	2
We outsource some security services to	Physcial security guard Private security company
We outsource most security services to	
I don't know	
<b>Q1.12 Is there a legal or regulatory framework that obliges your company to implement security measures, such as NIST or other national regulatory security obligations?</b>	
Yes	2
No	
Other(s) (please specify)	ISO27001, GDPR
I don't know	
<b>Q1.13 Does your Executive Committee participate in the definition of your company's cybersecurity strategy?</b>	
Yes	4
No	1
<b>Q1.14 Do you have in place agreements with other organizations (such as CERT) or companies (in the same field of operations or not) for exchanging cybersecurity and potential threats information?</b>	
I don't know	
Yes, for cyber security	3
Yes, for physical security	
Yes, for both (cyber-physical)	
No	
I don't know	2

<b>Q2.1 Do you possess a generic verbose description of your telecommunication system?</b>	
Yes, we have one and are willing to share it within the Resisto project	1
Yes, but we cannot share it	1
No	1
I don't want to answer	2
<b>Q2.2 Do you possess a graphical (e.g. SysML) description model of your telecommunication system?</b>	
Yes, we have one and are willing to share it within the Resisto project	
Yes, but we cannot share it	2
No	1
I don't want to answer	2
<b>Q2.3 Do you possess a geo-referenced model of your telecommunication systems?</b>	
Yes, we have one and are willing to share it within the Resisto project	1
Yes, but we cannot share it	3
No	
I don't want to answer	1
<b>Q2.4 Do you possess a real-time capable simulation model of your telecommunication systems?</b>	
Yes, we have one and are willing to share it within the Resisto project	
Yes, but we cannot share it	
No	2
I don't want to answer	3
Other	
<b>Q2.5 How many subsystems of your system (e.g.) would you consider relevant for the resilience analysis?</b>	
1-3	1
3-10	3
>10	1
I don't know	
<b>Q2.6 How many types of components (e.g.) would you consider relevant to specify your system in terms of functionality and interconnectivity?</b>	
1-3	
3-10	4
>10	1
I don't know	
<b>Q2.7. Does your company use cloud computing i.e. IaaS / SaaS / PaaS / DaaS products such as Office 365™, Salesforce™, App Cloud™? To what extent would you say your infrastructure is cloud-based as opposed to 'hard-iron', locally deployed datacenter-type infrastructure?</b>	



MOST of our services are cloud-based (i.e. – e-mail, CRMs, Virtualization, Social Networking, Task Management, Workforce Management, Development, Security Services, Automatization, Containerization etc.)	
SOME of our services are cloud-based	2
NONE of our services are cloud-based, ALL of our infrastructure is hosted in the Company's data center(s)	2
I don't know	1
<b>Q2.8 Are there standard-architectures your system use? (Please specify)</b>	
3GPP	1
ETSI	1
We follow certain standards such as ISO	1
I do not know	2
<b>Q2.9 Are there standardization agreements your architectures agree with, e.g. IEEE, IEC, ISO?</b>	
ISO	3
IEEE	1
I do not know	
<b>Q2.10 How do you define system boundaries?</b>	
I don't want to answer	2
Geographic / Spatial within device	
Function-wise	3
Hardware / Technology-wise	1
Spatial separation	
Other	
<b>Q2.11 How do you determine the interdependency of system components?</b>	
I don't want to answer	1
Geographic / Spatial within device	1
Function-wise	4
Hardware / Technology-wise	2
Spatial separation	
Other	
<b>Q3.1 Did you construct a list of system/service (non-)performance functions you would like to have monitored by the Resisto platform?</b>	
Yes	
Partially	2
No	2
I don't know	1
I can provide the list	1

<b>Q3.2 Did you construct a list of performance functions you would like to have developed by the Resisto platform to enhance overall risk control?</b>			
Yes			
Partially			2
No			2
I don't know			
I can provide the list			2
<b>Q3.3 Can you identify the relevant system components for each system function?</b>			
Yes, I have a detailed knowledge on how the system functions are affected by each system components			1
Partially, I have a rough knowledge on which components the system functions directly rely			3
No			1
I don't know			
<b>Q4.1 Which type(s) of security attacks has your company experienced?</b>			
Cyber			5
Physical natural			3
Physical man-made			2
Cyber-Physical			1
None			
I don't know			
<b>Q4.2 How exposed do you consider your company is towards security attacks (cyber, physical or combined cyber-physical)?</b>			
cyber	physical	cyber-physical	
3	1	-	very exposed
2	1	2	exposed
-	2	2	little exposed
-	1	-	not exposed
-	-	-	
<b>Q4.3 Which tools does your organization use to detect attacks?</b>			
Self-developed tools			3
Open-source software			2
Commercial products			5
None at all			

I don't know	
Other (please specify)	
<b>Q4.4 Your human-related security incidents fall into the following category:</b>	
Ex-employees	
Active employees	5
Ex-external consultants	
Active external consultant	1
Suppliers & partners	1
Customers	1
External attacks	5
Other (please specify)	
<b>Q4.5 Which are the most common triggers for activating security measures?</b>	
User complaints	2
Detection by internal tools/security equipment	5
A CSIRT / a private or national CERT	5
Other (please specify)	
I don't know	
<b>Q4.6 Do you have a mechanism or a communication channel where internal users such as staff or consultants can report incident to you?</b>	
Yes	4
No	1
I don't know	
<b>Q4.7 If you experienced an attack, who would you turn to for help?</b>	
We would solve it internally	5
A security consultant	1
A telecom operator	
A hardware or software security vendor	
An IT provider	
A local authority / national CERT	1
Other (please specify)	
I don't know	
<b>Q4.8 Do you maintain and regularly updated threat and disruptions lists?</b>	
Yes	3
No	2
I don't know	
<b>Q4.9 Which tools do you use for threat list maintenance and updating?</b>	

N/A / None	2
I do not want to say	1
<b>Q4.10 Can you provide a pre-assessment of threats independent of their targets?</b>	
Yes	3
No	2
I don't know	
<b>Q4.11 How do you assess the correlation between threats (coincidence, potential cascading)?</b>	
We do not assess correlations	1
We assess correlations via:	Internal tool
	Internally developed systems using Open source and vendor solutions
I don't know	2
<b>Q5.1 On overall, on a scale from 1 to 10, how do you evaluate the IT security level of your company? (1 means that you judge your company as not protected at all and 10 means that you judge your company as highly protected. The scores in between allow you to refine your judgment).</b>	
1	
2	
3	
4	
5	
6	
7	
8	4
9	1
10	
Comments:	
<b>Q5.2 On overall, on a scale from 1 to 10, how do you evaluate the physical security level of your company? (1 means that you judge your company as not protected at all and 10 means that you judge your company as highly protected. The scores in between allow you to refine your judgment).</b>	
1	
2	
3	
4	

5	1
6	
7	1
8	2
9	1
10	
Comments:	
<b>Q5.3 On overall, on a scale from 1 to 10, how do you evaluate the cyber-physical security (both modalities at the same time ore in close interconnection) level of your company? (1 means that you judge your company as not protected at all and 10 means that you judge your company as highly protected. The scores in between allow you to refine your judgment).</b>	
1	
2	
3	
4	
5	
6	1
7	1
8	3
9	
10	
Comments:	
<b>Q5.4 How do you assess the criticality of threats?</b>	
Empirical data driven	2
Expert rating	4
Tabular Hazard Analysis-like approach	2
Other (please specify)	
I don't know	
<b>Q5.5 How do you assess the relevance of threats for performance functions?</b>	
Empirical data driven	
Expert rating	2
Tabular Hazard Analysis-like approach	2
Other (please specify)	
I don't know	
<b>Q6.1 Do you use a Security Information and Event Management (SIEM) Solution?</b>	
Yes, a commercial solution with support	4
Yes, an open-source solution	
Yes, a custom-made solution developed in-house	

No	
I don't know	1
<b>Q6.2 Does your company operate a Security Operations Center (SOC) for real time threat assessment?</b>	
Yes, we have a SOC facility on-site	3
Yes, we outsource it to a MSSP / third party	
No	2
I don't know	
<b>Q6.3 Does your SOC / SIEM solutions use Big Data technologies for monitoring and event log and event criticality analytics?</b>	
Yes	3
No	2
I don't know	
<b>Q6.4 Does your company perform cyber-security audits such as pentests?</b>	
Yes, we conduct the audits internally employing cyber-security staff using red team / blue team exercises	
Yes, we conduct the audits internally using automated software tools for auditing and reporting	5
Yes, we outsource it to a third party	
No	
I don't know	
<b>Q6.5 Does your company have a Security Model and/or simulation for risk assessment and management of Cyber-Physical Systems?</b>	
No, we don't integrate Cyber Security and Physical Security Systems	3
Yes, we use a well-documented model such as Expert Elicited Model, Attack Graph Method, Game Theoretic Model(s), Petri Net, Stochastic Games	1
I don't know	1
Other (please specify)	
<b>Q7.1 Which factors determine whether a risk is considered acceptable?</b>	
Economic	4
Press, media echo	2
Technology driven	4
Other (please specify)	Severity
<b>Q7.2 Which risk and resilience evaluation criteria are in place?</b>	
Risk management/Business Impact Analysis	1
I do not know	2

<b>Q7.3 How should risks and resilience level be communicated?</b>	
Top management meetings	1
Internal communications and intranet sites	1
I do not know	1
<b>Q8.1 Have you implemented a process to select the best technology solution to control non-acceptable risks or to improve the resilience for such risks?</b>	
Yes	4
No	1
I don't know	
<b>Q8.2 How do you compare different technology solutions?</b>	
By running simulations e.g. of the networks	
By expert recommendation or external company consulting	1
By direct implementation and on-site testing	5
Other (please specify)	
<b>Q8.3 Which information would be useful to manage a hazard easier?</b>	
Affected components / systems	4
Affected system functions	4
Components/system linked to the affected components/systems	4
Historical/empirical data on similar events	3
Real time simulations of the events	2
Other (please specify)	
<b>Q8.4 How should this information be displayed/delivered?</b>	
Tabular/text based web interfaces	2
Grafical based web interfaces	5
Other (please specify)	
I don't know	
<b>Q8.5 Which software tools would be useful for an improved decision-making process?</b>	
Risk management software	5
Other (please specify)	
I don't know	
<b>Q8.6 In case your company is operating Industrial Control Devices (ICD) based critical Infrastructures (CI), are there any best practices on securing the operations of those infrastructures?</b>	
No, we are not operating ICD based CI	2
Yes, basic security in place based on segregation between IT network and operational network	1

Yes, based on Commercial security solutions	2
Yes, based on in house developed security solutions	
I don't know	
<b>Q8.7 Does your company address the emerging security threat in the 'Internet of Things' (IoT) and/or Industrial Control Devices (ICD) era?</b>	
We have a proactive stance on IoT/ICD with a well-defined cyber-security life cycle - we inventory, assess, patch and test all of the IoT/ICD devices deployed in our corporate networks	2
IoT/ICD Security is not a priority, the connected devices in our networks are treated just like any network-active device (i.e. Wireless routers)	1
Not applicable - our company does not deploy any devices in the IoT/ICD category	1
I don't know	1
<b>Q8.9 Do you consider that your company needs to allocate effort in defining / updating its digital security strategy to evolve at the same pace as the many new developments in the new digital era?</b>	
No	
Yes, triggered by the massive adoption of the virtualization and software defined network (SDN) technologies	3
Yes, triggered by the 5G adoption including the new roles such as Cloud operator, Infrastructure operator, Digital Application provider, Digital Application User	5
Yes, triggered by the 5G IoT adoption	4
Yes, triggered by the adoption of the soft SIM (subscriber identification module) where the device will not have any SIM hardware at all, the SIM functionality will be delivered onto the device virtually, or over the air once the user switches it on	2
Yes, triggered by the adoption of the artificial intelligence (AI)	3
Yes, triggered by the adoption of the machine learning	3
Yes, triggered by the adoption of the blockchain technology	2
Yes, others (please specify)	
<b>Q8.10 Blockchain technology could provide interesting prospects for developing blockchain-based solutions for cyber security applications in various verticals that deal with asset protection including IoT/ICD devices an CI (Critical infrastructure). Do you see any benefits in adopting such approach for your company and/or critical infrastructure protections?</b>	
Yes	5
No	
I don't know	
<b>Q9.1 Do you correlate CCTV / physical intrusion detection system data with IT security incidents?</b>	
Yes, automatically	1
Yes, manually	3
No	



I don't know	1
<b>Q9.2 Does your company set up trainings for employees regarding IT security risks and recommended behaviours?</b>	
Yes	5
No	
I don't know	
<b>Q9.3 The personnel in charge with Security activities in the company is sent periodically (at least once a year) to perfection/training sessions?</b>	
Yes	5
No	
I don't know	
<b>Q9.4 Which of the following IT Security solutions and technologies do you use for your company (multiple answers possible)?</b>	
Instruction Prevention Systems	4
Next Generation Firewalls (NGFWs)	4
Distributed Denial of Service (DDoS) Mitigation (Protection) Systems	5
Web Filtering	4
E-Mail Security including Anti-S	5
Data Leakage Prevention solutions	2
DNS Filtering	5
End-Point Protection for fixed (i.e. workstations) solutions including Anti-Malware software on endpoints	4
End-Point protection for mobile (i.e. laptops, smartphones, tablets) solutions including Anti-Malware software on endpoints	4
Web Applications Filtering	4
Others (please specify)	
I don't know	
<b>Q9.5 Do you use any cloud-based security solutions and/or services? If so, please list such solutions below: (i.e. - Cloudflare's Anti-Ddos, Fortinet's MultiCloud etc. Zscaler's Cloud Security etc.)</b>	
No	2
Fortinet's MulitCloud	1
Not sure	1
<b>Q9.6 Does your company have a Remote Access policy applicable to remote users such as employees or consultants?</b>	
Yes, remote users can access the infrastructure only trough VPN (IOSec, SSL) connections	5

Remote users can access their e-mail from the internet but cannot access the infrastructure from outside the local network	
Remote access is prohibited altogether, users have to be inside the perimeter to access any of the company's resources	
I don't know	
<b>Q9.7 Does your company have a 'Bring Your Own Device' (BYOD) Policy in-place? (check all that apply)</b>	
Personal devices are permitted on the premises but may be used only as isolated 'guest' network	2
Personal devices are permitted on the premises and are used to access the Company's information and applications (POCE or 'Personally owned, company enabled')	1
Users are issued with company-owned devices such as laptops and mobile phones that are enabled for both business and personal usage (COPE or 'Corporate Owned, Personally Enabled')	3
Personal devices are NOT permitted on the premises, users may access corporate resources only via the fixed devices (i.e. workstations) issued by the company	1
I don't know	
<b>Q9.8 Does your authentication mechanisms for your sensitive applications, addressed to your employees, customers or suppliers, use complementary factors (biometrics, one time password, etc.) to the password?</b>	
No	2
Yes, biometrics	
Yes, with at least two factors (one time password, PKI,...)	3
I don't know	