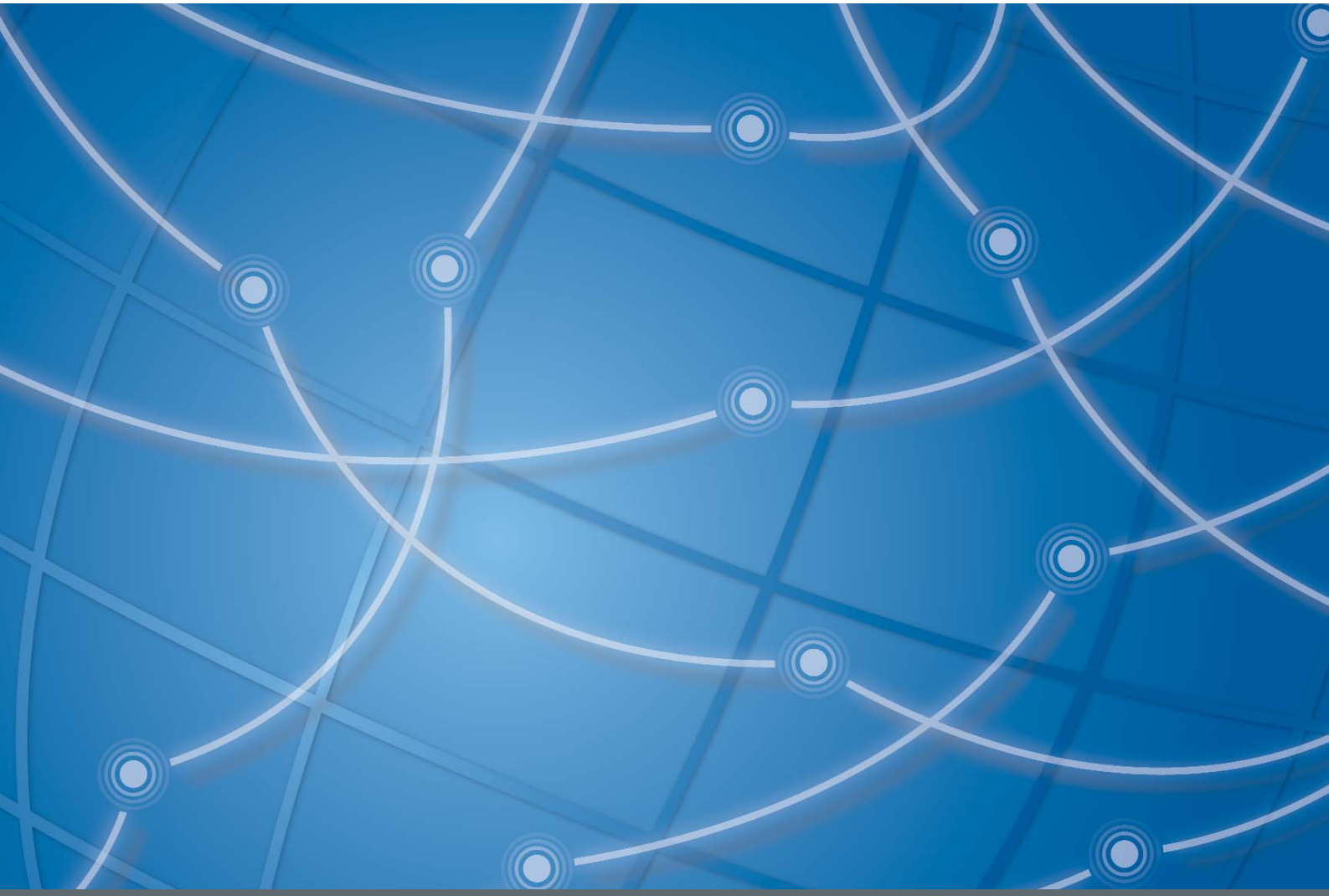


# Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations

enisa
European Network and Information Security Agency

## About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

## Acknowledgments:

While compiling this report, we talked extensively over a period of many months to a large number of technical and managerial staff at communications service providers, vendors, and service users (Annexe C - List of respondents / contributors). ENISA would like to express its gratitude to the stakeholders that provided input to the survey.

Many thanks also to the Deloitte team that helped to gather the material and supported the drafting of this report.

## Contact details

For more information about this study, please contact:
Dr. Panagiotis Trimintzios
Network Resilience and CIIP
ENISA
panagiotis.trimintzios@enisa.europa.eu
http://www.enisa.europa.eu/act/res

## Legal notice

# Table of contents

# List of figures

# Executive summary

# Executive summary

ENISA's program on Networks and Services Resilience and Critical Information Infrastructures Protection (CIIP) has been central to recent policy initiatives in the European legislative environment. Within that program, the assessment of practices and policies to improve the level of resilience has been deemed a critical aspect. As a step towards a uniform assessment of resilience across Europe, a project has been started to identify resilience metrics and measurement frameworks for public communications networks.

This report documents a part of that study, where **stakeholders were surveyed on the challenges and recommendations for resilience metrics** (see Annexe B – Survey questions). The survey was conducted among experts in various sectors (academia, regulators, policy makers, standardisation bodies and private organisations) who provided input both in writing and by interviews.

The goal was to **collect information on existing practices and metrics** with key experts and stakeholders and to perform a **qualitative analysis of the input** received. This non-technical report provides an **overview of the results for policy experts** in the area of resilience.

The results in this report are structured in two sections. The first section summarises the main challenges that were identified by the stakeholders. The second section outlines a number of recommendations on how to overcome these challenges. At the end we present the detailed feedback received from the stakeholders.
The most important challenges identified were:

- **The lack of a standardised framework**, even for the most basic resilience measurements. There are not that many frameworks available and none of them are globally accepted
- **No standard practices** were identified within the different organisations for the baseline resilience metrics. Different organisations all use their own specific approaches and means of measuring resilience, if they measure at all. This impedes the usage of those metrics for overall assessment of resilience, or the aggregation and composition towards higher levels (such as a national or a pan-European assessment of resilience)
- **Lack of knowledge and awareness of resilience metrics**. This results in severe difficulties for organisations when deploying resilience metrics

To improve on the current state of resilience metrics, a number of recommendations emerged from the analysis of the information received during the online survey and the interviews with participants:

- The European Commission and the Member States should create a **common understanding and good practices or standards** on resilience metrics
- The European Commission and the Member States should **stimulate investment** in the research of resilience metrics and measurements open issues
- The European Commission and the Member States should **increase the awareness** of resilience metrics and the relevant regulations related to resilience
- The European Commission and the Member States should support the **development of automated tools** to help the deployment of resilience measurement (mainly data collection and data analysis)
- The European Commission and the Member States should **facilitate and encourage the sharing of information and good practices** in resilience metrics. The creation of closed, or sector-specific information sharing, groups could increase the level of trust required for organisations to share information
- Regulators, industry consortia and public private partnerships should **create clear and practical guidelines** on the measurement of resilience, including its interrelationship with applicable legislation

# Introduction

# Introduction

Attacks on the Internet, disruptions due to physical natural phenomena, software and hardware failures, technology obsolescence and even human error may all affect the proper functioning of either public or private communications networks and of related or supported services. Such disruptions reveal the dependency of our society on these networks and the services they support and the interdependency of systems when they interact with each other.

Network resilience becomes more and more important to security and risk theory, applied practices and policy decisions. The concept of resilience is gaining ground with many involved stakeholders and several definitions and conceptual approaches to resilience have already been adopted.

A well defined and accepted system of metrics and measurements is essential in order to assure the desired resilience of networks.

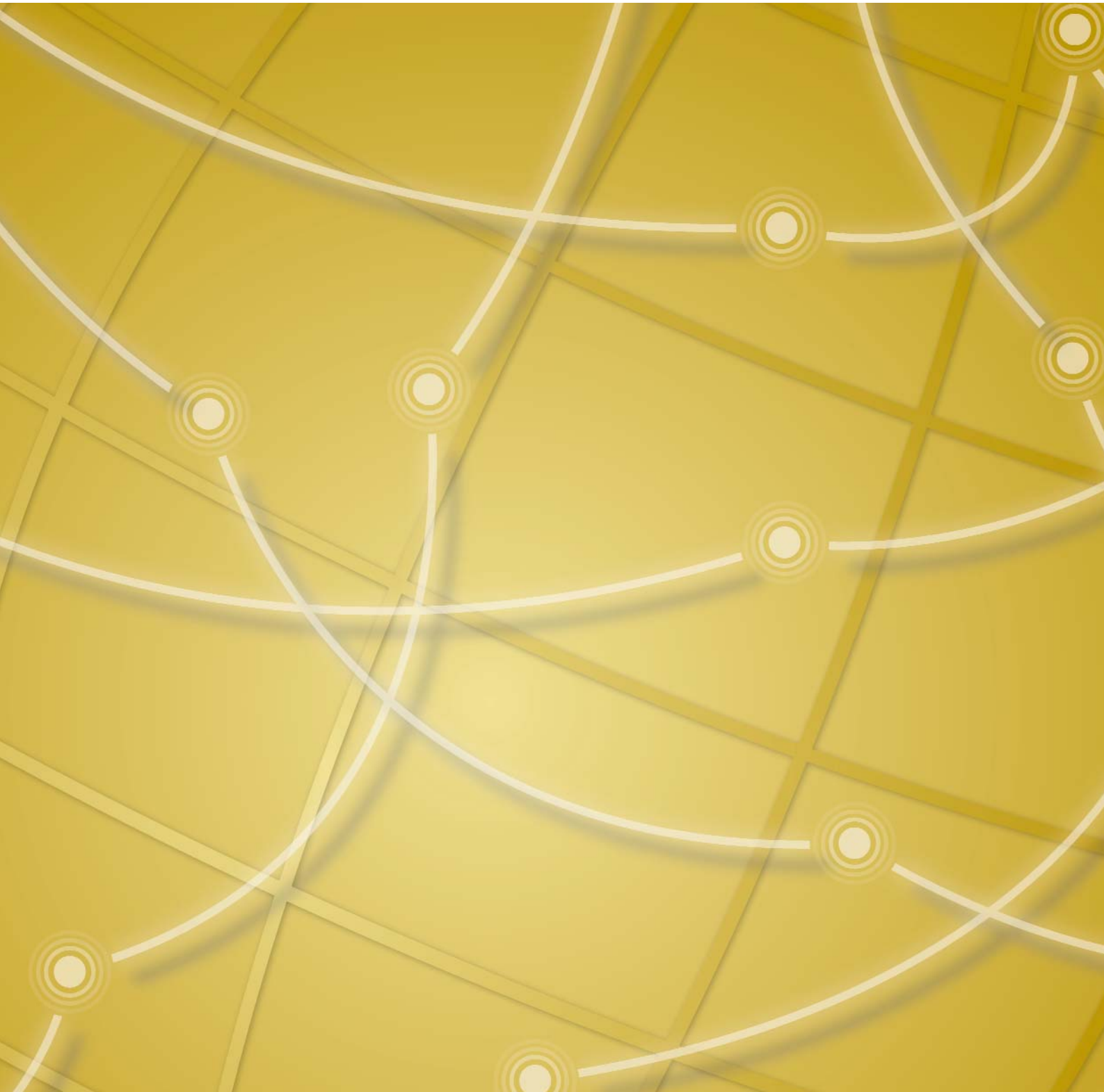
However, even the basic resilience measurements performed today are still lacking a standardised framework, or widely accepted set of good resilience metrics. The maturity level of the current metrics frameworks is in marked contrast to the complexity of and dependence on communications networks as a whole.

As part of the study supervised by ENISA, a set of metrics-specific questions (see Annexe B - Survey questions) was sent to a group of stakeholders. These questions concerned how resilience is measured on a sector basis (the surveyed participants were from public and private organisations, as well as national regulators, academia, etc.). The overall methodology is described in Annexe A.

This document presents the results of that study and aims to provide a non-technical overview to policy experts in the area of resilience. The key challenges to resilience measurements and the most interesting aspects of the answers received are summarised and analysed in this document. This report also summarises a number of recommendations arising from the analysis of the information received.

The rest of the report is organised as follows. Section 2 presents the main challenges impeding the adoption of a commonly accepted framework for resilience metrics and measurements. In section 3, we summarise the main recommendations for future actions in the area of network and service resilience metrics and measurements. Finally section 4, includes all the detailed input we received from the questionnaires and interviews with stakeholders.

# Challenges



# Challenges

Following the ENISA survey[1] launched in the first part of 2010, responses were collected, analysed and subjected to a qualitative analysis.

A large part of the input received during the survey and interviews consisted of the different challenges in measuring resilience, as encountered by the respondents. This section presents the most interesting aspects of that input, grouped in two major categories.

## Main consensus points

**A lack of standard practices[2]:** despite the variety of the surveyed stakeholders, we expected to find systematic patterns in how resilience is defined and measured and in the frameworks and metrics that are used. Unfortunately, it was not possible to point out standard practices that stakeholders are using in this area: organisations use their own specific approaches and means of measuring resilience, if they use any at all.

Organisations report major hurdles in the identification and implementation of adequate metrics or measurement frameworks, either because the metrics do not exist, or because the organisations are unaware of their existence. In general, maturity of current practices is low.

Difficulties in deploying: A **lack of knowledge and awareness** impedes further deployment of resilience metrics.

**More analysis**, long and active **co-operation** is needed in order to achieve common understanding and approach.[3]

**The use of measurement frameworks and metrics is beneficial[4]**, especially when applied as a process, where improvements to the collection and usage of metrics within organisations are made in an iterative manner, based on the experience gained from the use and analysis of historical data.

**The usefulness and value of metrics is challenged when complexity increases[5]:** in cases where relevant measurement data is difficult to collect, or when its analysis becomes too complex and subject to interpretation, the usefulness of resilience or security metrics was severely challenged. Focus on the key issues in resilience measurement is seen as important and there is also a clear need for tools and solutions to rationalise the measurement data overload.

**Drivers for resilience metrics[6]:** on the other hand, there are several specific and commonly recognised needs and drivers for adopting resilience (and security) metrics and frameworks, such as:

- The need to show and provide **assurance** and evidence on the level of resilience and/or security achieved
- Validation of conformance with regulations, policies and business requirements
- The practical need to analyse in an effective and efficient manner the increasing number and complexity of technical logs

1 We refer to the ENISA survey questionnaire used for this study. See Annexe B - Survey questions.
2 See section: Measuring resilience and security, page 18 and Problems and suggestions - Key unsolved problems in assessing, measuring, and benchmarking the security and resilience of networks and services, page 33
3 See section: Overview and general comments, page 17 and Measuring resilience and security, page 18
4 See section: Measuring resilience and security, page 18
5 See section: Measuring resilience and security - Data sources, page 21
6 See section: Measurements , page 24

**Preference towards a conservative approach in introducing metrics**[7]**:** even if resilience (and security) metrics are in general well-defined, not all of them are feasible for practical use, due to a variety of reasons. Most respondents agree that the most reasonable approach to introducing resilience and security metrics should be to start with a small set of metrics, which should follow the key principles below:

- Start with a small set of metrics. These should be clearly defined, meaningful and generally accepted metrics
- Focus on specific systems and services
- Consider data availability constrains and complexity
- Define and refine thresholds based on several measurement periods, not as an absolute value upfront
- Review and evaluate metrics on a regular basis: they should not be static and organisations should not be afraid to abandon metrics if they prove to be of little added value

## Other important points

In addition, we received a number of important points on which there was not necessarily a consensus. The most interesting ones are considered below, grouped in relevant categories:

*Challenges in defining or selecting appropriate measurement frameworks and metrics*

- **Resilience is not a well-defined or understood term**[8] and, depending on the context, it encompasses several interpretations and viewpoints. A common point of disagreement is whether security and resilience should be seen as two different, loosely-coupled concepts or whether security should be viewed as an integral part of resilience
- Although it is recognised that the **resilience and security of the systems and services is improving as a direct or indirect result of using measurements**, these **improvements are not always reflected or captured by the metrics**[9]. Measuring security incidents serves as an excellent example; it is very hard to objectively measure improvements of defences against security incidents (in other words: to show what might have happened if certain security mechanisms were not improved)
- **Insufficient organisational buy-in**[10], especially if the resilience is not a specific or high priority business requirement, or when the resources required to measure resilience are not considered (e.g. since the design phase of the implemented systems or services)
- In general, there are **only few cases where regulations, guidelines or administrative provisions exist**[11] relating to the adoption or interpretation of measurement frameworks, or metrics for security or resilience. Most stakeholders are looking towards the CERTS, national regulators or industry associations for guidance in this area
- Problems are more difficult to overcome, especially in the **setup phase** of measurements where the boundaries of system/service and the measurement thresholds must be defined and the dependencies be identified
- Even greater difficulty lies in **matching resilience and security requirements**[12] to be achieved (such as a 99,9% service availability requirement) to a metric (such as number of single points of failure contained in the service), or to a specific risk

7 See section: Measuring resilience and security, page 18
8 See section: Measuring resilience and security, page 18
9 See section: Analysis and risk management - Metrics as an iterative tool for security and resilience managers to periodically evaluate the effectiveness of various components, page 27
10 See section: Strategy and governance - Measuring resilience and security, page 18
11 See section: Collaboration and information exchange - Initiatives between authorities, private sector, academia, or other stakeholders to align efforts regarding security or resilience metrics, page 29
12 See section: Models, formulas or tools used in the analysis of the measured quantities, page 28

*Challenges in applying measurement frameworks and metrics*

- **Separate functions responsible respectively for resilience and security**[13]: although resilience and security are usually seen as a whole from a conceptual approach, in practice there are cases where there are two (or more) separate functions responsible for resilience and security respectively. Usually, this implies misalignments, different approaches, or a lack of focus and results in separate sets of metrics or different frameworks being used. This mostly happens due to the fact that security and network engineering are positioned as different professions within the same organisation

- **Lack of readily available tools/solutions**[14]: although most stakeholders are actively measuring the resilience and/or security of their networks and services - albeit by using availability as a general metric - all stakeholders confirm that no readily available tools/solutions for measuring resilience and security exist

- **Information sharing barriers**[15]: a recognised limitation in applying resilience measurement frameworks and metrics has its root causes in the relatively limited information exchange on current good practices. Some **categories of organisations have a strong culture** and tendency to avoid transparency and they protect the information on their level of maturity and expertise in this area. In many cases they are simply declining to comment on security and resilience positions and practices

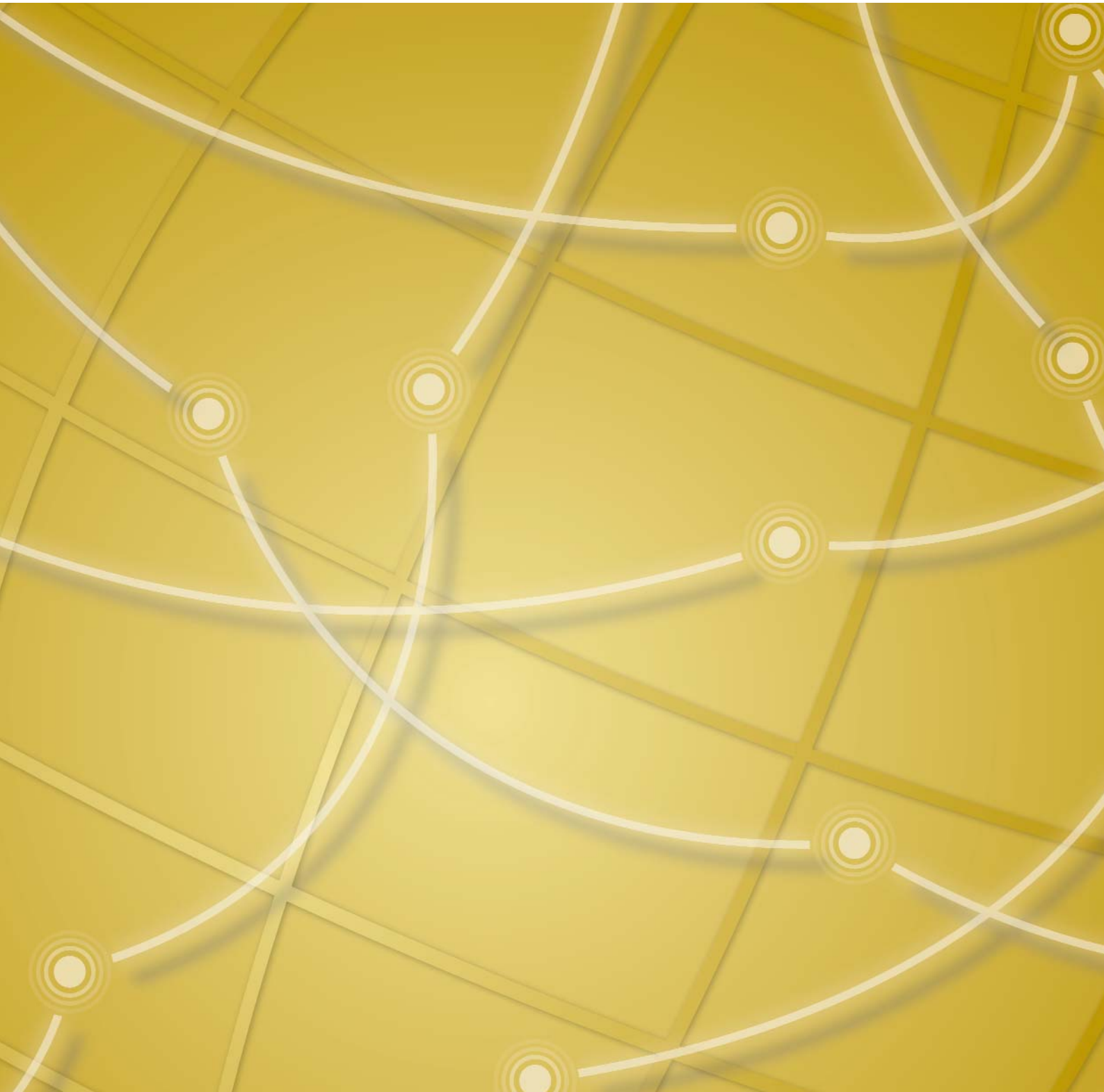
- **Not all resilience domains are considered**[16]: while many organisations are actively measuring availability, other concepts like reliability (i.e. the probability that a system or a network will perform its required function for a specified interval under stated conditions). are not always sufficiently taken into account in practice. Many stakeholders acknowledge that the use of availability metrics in a broader scope is well understood and applied while security metrics are considered to be much more opaque and difficult to define. Usually, the decision to limit the measurements to availability is a self-imposed limitation

Although all stakeholders agree that there exist today many challenges in defining and using resilience metrics, there are efforts to support the organisations in their implementation of metrics. A few cases where suggestions and good practices are shared on resilience and security metrics, measurement frameworks and the related reporting were reported.

They are provided in a transparent and open manner – typically they come from the CERTs, regulators, academia, or via the professional associations. Sometimes, this information sharing goes into detail[17].

13 See section: Problems and suggestions - Other limitations, page 32
14 See section: Problems and suggestions - Technical limitations, page 31
15 See section: Collaboration and information exchange, page 29 and Problems and suggestions, page 31
16 See section: Measuring resilience and security - Resilience, page 19
17 See section: Collaboration and information exchange, page 29 and Problems and suggestions, page 31

# Recommendations



# Recommendations

The previous section clearly outlined that the participants in the study considered the measurement of resilience to be a difficult and challenging issue. They agreed that the maturity level of current metrics frameworks was in marked contrast to the rapidly growing complexity of communications networks.

While the known challenges are considered to be serious obstacles to the implementation of resilience measurements, all respondents acknowledged the benefits of measuring resilience.

To improve the current state of resilience metrics, a number of recommendations emerged from the analysis of information received during the consultation with stakeholders. These recommendations are an attempt at defining areas where more work is needed to accelerate the adoption of resilience metrics:

- It is critical that a **common understanding and good practice or standard for resilience metrics** is created, which will enable different parties to speak a common language. Information and best practice sharing will benefit, as will the adoption rate of the resilience measurements discipline. The need for a common understanding is also emphasised by the different generally recognised drivers:
  - The need to show and provide assurance and evidence on the level of resilience achieved
  - The need for a metrics system for validating the conformance with regulations, policies and business requirements
  - The practical need to analyse in an effective and efficient manner the increasing number and complexity of technical logs
  - Development of software tools (see also the next recommendation) can also be accelerated when based on common, accepted, standardised definitions

For example, this could be achieved by standardisation bodies, or by co-operation between different regulators or authorities.

This common understanding should be based on a commonly accepted, high-level taxonomy of resilience metrics, as well as with a minimum set of baseline resilience metrics. The metrics should include descriptions of the related measurement method, the measurement unit, the objective of the metric and how the metric will quantify the impact of a possible failure.

- **Further investment in the research and development of resilience metrics** open issues must be made to pave the way towards adoption and implementation of resilience metrics on a wide scale. The main open issues identified are:
  - **Aggregation and composition:** unresolved issues exist when one wants to combine metrics used within a single corporation to gain insight into the resilience status at higher levels of abstraction. This becomes even more difficult when we cross the boundaries of a single corporation/organisation. When, for example, we want to assess the resilience status beyond the levels on a sector-wide basis, on a national basis or even on a pan-European level, it becomes virtually impossible
  - **Setting the scaling and the thresholds:** it is important to have a scaling and thresholds for each metric. The scaling will give a granular representation of the measured metrics, helping to quickly identify the status. Finding and setting the thresholds for a scalar representation is a very difficult task, which might not have a perfect (fits all) solution. Indeed, though difficult, it is important to understand the factors that have to be taken into account when setting those thresholds that identify the service level transitions to different states (e.g. the minimum acceptable service level)

  - **Data analysis for prediction and forecast modelling:** extensive data analysis is required to transform metric values into network resilience insights, especially for more complex metrics and environments. It is important that models for forecasting and predicting are studied, developed and used

- **The awareness of resilience metrics and good frameworks must be increased:** only after organisations become knowledgeable about the metrics field and its benefits will implementations start to take place. The creation of awareness should be accompanied by references towards good frameworks, in order to guide organisations

- The development of **software tools** can lower the barrier to the challenges currently experienced in **data collection and analysis** – the tools could automate the deployment of resilience measurements

- The different regulators should create clear **and practical guidelines** for the measurement of resilience and should **increase the awareness of different regulations**

- **Co-operation** between countries, public and private organisations should be facilitated and **the good practices and information sharing** in resilience measurements encouraged. National or industry CERTs can play a major role in the information sharing process.

There are some categories of organisations where a strong culture and tendency exists to avoid transparency and to protect the information on their level of maturity and expertise in this area. A first step for these organisations could be to co-operate in **closed and sector-specific information sharing groups**, to lower the entrance barrier and to avoid the sharing of information with unwanted entities

- The **good practices must be developed**, become **available** and their application supported among the others by raising awareness

- When starting on measuring resilience, an organisation should begin by using a small set of metrics, following these **key principles**:

  - Metrics should be **clearly defined**, meaningful and generally accepted

  - Focused on **specific systems and services** and taking into account the boundaries of those systems and services

  - Taking into consideration **data availability constraints and complexity**

  - With **thresholds defined and refined** based on several measurement periods, not as an absolute value upfront

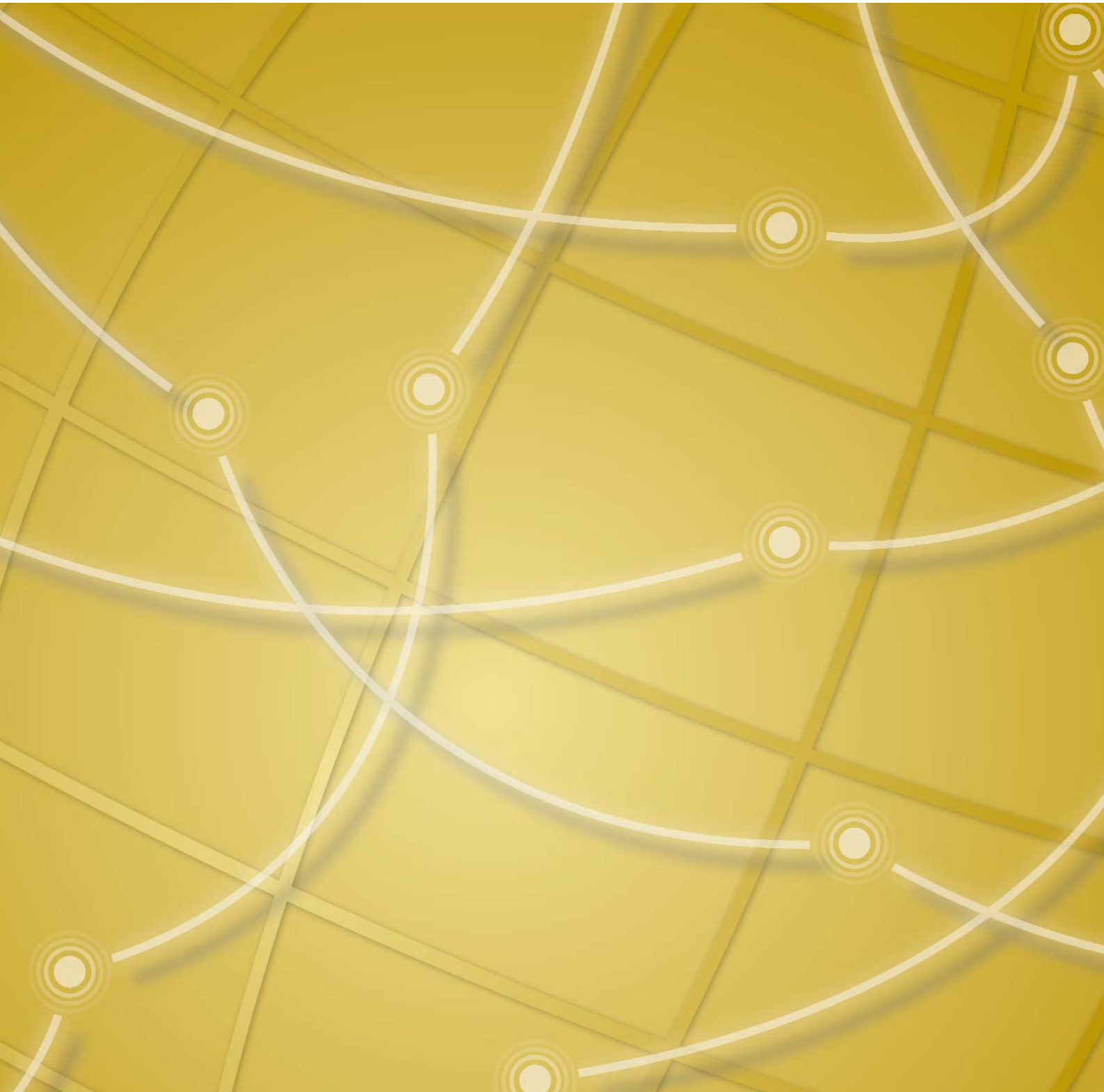
  - Metrics should be also **reviewed and evaluated on a regular basis:** they should not be static and organisations should not be afraid to abandon metrics if they prove to be of little added value

- When matching resilience and security requirements to metrics, care should be taken that these requirements can be translated into **realistic and objectively measurable metrics**. This step should be considered as an **iterative process**, not as a one-time mapping. Metrics should reflect variations in the resilience property under measurement in an unambiguous manner

- When implementing resilience metrics, **sufficient buy-in** from all parties should be assured. Insufficient organisation buy-in has been described as a challenge, but a lack of resources for collection and analysis could also inhibit the implementation's success. The **measurement of resilience should also be an iterative process:** more than integrating the metrics in a dashboard, it requires follow-up and fine-tuning

- There is no consensus on whether security is a part of resilience, or should be considered as a separate domain. As a consequence, there are cases where separate functions are responsible for resilience and security respectively. In these cases, **sufficient buy-in from security** should be acquired before implementing resilience metrics. This will avoid misalignments and double measurement implementations

# Analysis of findings – details



# Analysis of findings – details

The split of surveyed stakeholders, by category, is depicted in Figure 1.

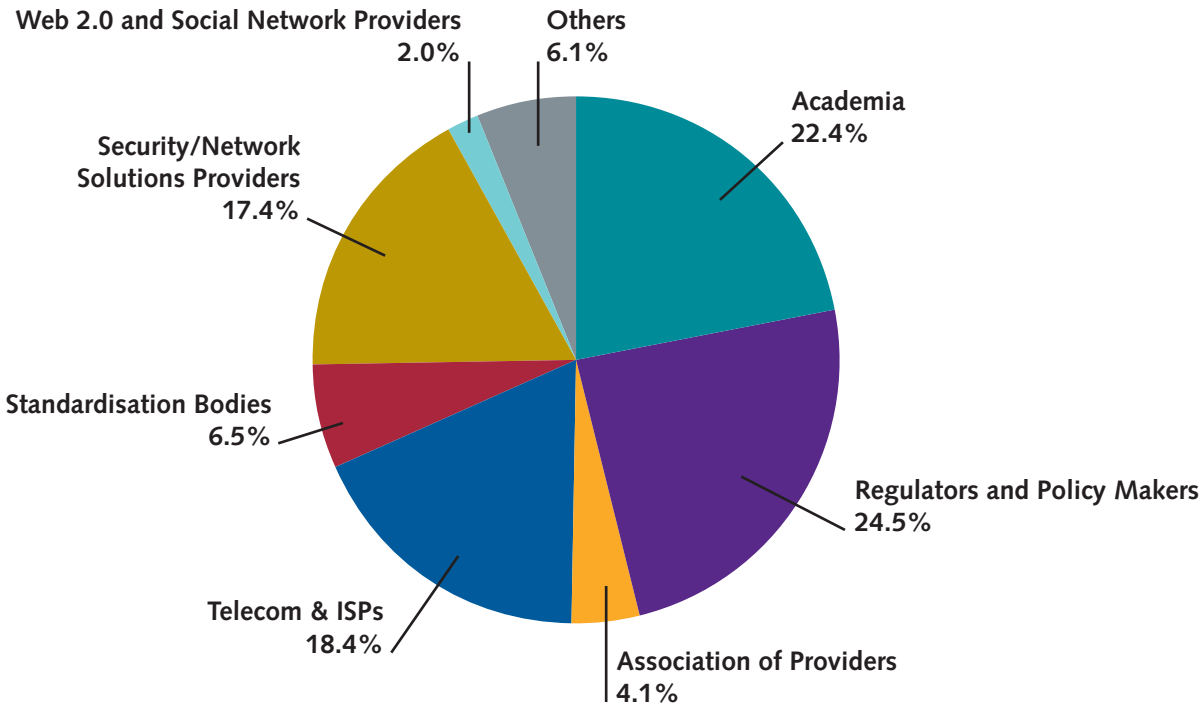



Figure 1: Split of surveyed stakeholders

## Overview and general comments

The first observation made after receiving the initial survey responses concerned the major differences of opinion among organisations from different sectors and countries on the very basic concepts and characteristics of metrics and measurement frameworks for the resilience and security of communication networks and services.

In many cases, there was even a confusion of terms that can be easily interchangeable when discussing measurements, metrics, measures, indicators, etc., which was observed during the survey and is also acknowledged by other independent research [1]. No particular preference was noted towards the term 'measurement' in comparison with 'metric'.

All stakeholders declare they understand the concepts of resilience and security and agree that these concepts are not identical, or that they have major differences, depending on the organisation. However, the common denominators, such as service availability and incident management, are not new to the stakeholders.

We illustrate below some of the most relevant differences:

- Definitions and concepts used vary significantly, case by case, for instance:
  - Name of the metric and the underlying notion it is supposed to address/capture
  - Identified/known problems with the definition of the metric, or due to the expected errors
  - Standard unit of measurement used
  - Definition of the complex metrics used (composition of two or more basic metrics)

- Assignment of roles and responsibilities for measuring the resilience and security aspects is very diverse – from very formalised cases to ad hoc – with a higher level of maturity in definition of responsibilities noted in relation to security

- Very few, and rather ad hoc metrics are used for measuring resilience aspects, while security metrics are more refined, including composed metrics – i.e combinations of baseline metrics
- There is a mix of analytical and empirical metrics that are considered or used in practice; however there is no clear path or preference noted. The analytical type appear to be easier to define (and to be adopted), but in reality they do not always help in defining measurement methodologies, or lead to development of related or future metrics
- There is interest among the surveyed stakeholders in benchmarking possibilities and the use of more standardised metrics, with relevance to the type of organisation they represent – this is sometimes against the common preference for very specific and customised metrics
- A major challenge remains the way in which the degree of resilience and security can be quantified and measured in an objective way, making it more tangible

*'The mere notion of 'resilience' is as yet undefined in most situations, and more research should be undertaken to firmly place it on the agenda. Similarly to information security in the 1990s, business resilience and related metrics (or maturity assessments) are in their infancy as a professional discipline...'*
**Quote from a surveyed regulator**

## Strategy and governance

**Measuring resilience and security**
When asked how resilience and security were measured, it became clear that organisations had a different understanding and use of the concepts and definitions involved. Also, they had (in some cases) opposing views on the need to adopt and effectively use measurement frameworks and metrics. The usage of measurement frameworks and metrics is presented in Figure 2.

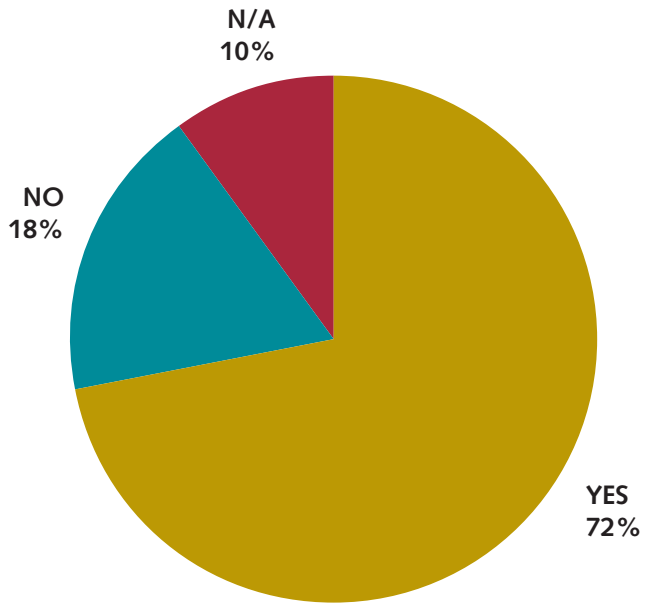



**Figure 2: Stakeholders measuring resilience and/or security**

The survey participants generally agreed on the importance of and the benefits to be gained from measuring resilience and security. However, there are still multiple obstacles to overcome, most of them related to internal organisational constraints; unclear responsibilities, lack of resources and tools, difficulties in getting buy-in for the defined metrics, unreliable data etc.

Maturity of current practices for measuring resilience and security is generally acknowledged as being very low, although the organisations involved did not specifically indicate the reasons behind this statement, or the manner in which they assessed it. One stakeholder reported the use of a number of approaches and frameworks produced by the research community to address the maturity of security in his organisation[18].

Some key drivers for measuring resilience and security are:

- Reporting and compliance requirements (internal, from regulators or customers)
- The need for better and more effective controls
- Operational and design improvement requirements for the infrastructure, services and processes involved

In many cases, the responsibility for measurements is conferred by law, or by regulation assigned to the network operators, ISPs, etc. In general, they have well defined functions for measuring resilience or security, and these are implemented in order to ensure compliance with the regulatory requirements.

#### 1.1.1.1 Resilience

With respect to the commonly accepted metrics for resilience, availability and reliability is the most used, showing respectively the extent to which the system or service involved is available whenever it is required, and the extent to which the service continues to be provided during the period that it is being used.

Availability is considered to be an all-encompassing resilience metric; downtime, response time and repair time are in general considered to be embedded in the availability records. Its popularity also derives from the simple manner it can be defined and modelled with respect to such components as the (network) element that is measured, the resilience objectives against which the element is measured and the method used to measure it.

The most cited '**operational**' resilience metrics are:

- Steady-state availability - however in defining and using this there are additional aspects to be considered. Availability (or non-availability) metrics can differ significantly when the impact of an outage is considered as well, depending for instance on the population in relation to which the availability is measured. Organisations may, for instance, define a service or system as 'up' when it is available to 99% of the users, or running at least at 90% capacity. The percentages used are very important when it comes to the definition of availability and they may significantly differ, case by case
- Performance of the network service, such as available bandwidth and the round trip time measured between two fixed points in the network
- Mean time to repair (MTTR): the (average) time elapsed until service restoration after an incident, or a major interruption, has taken place

18 The following were quoted: Systems Security Engineering Capability Maturity Model SSE-CMM (ISO/IEC Standard 21827); INFOSEC Assessment Capability Maturity Model IA-CMM; Information Security Program Maturity Grid and Murine-Carpenter Software Security Metrics.

- Network down time (also referred to as outage time) is equal to the amount of time that the network service was not available from the end user's viewpoint. This can, but does not have to, match with the MTTR - in a redundant network, a backup system can and will take over the functions from the primary device, resulting in service restoration. While the service would again be considered as available by the service consumer, the primary router might not yet be repaired (and thus is still counting on the MTTR)

- Time of response: the time between the detection of an incident or interruption and the first remedial action taken in order to restore a desired level of service, availability, etc.

- Number and duration of incidents with impact on the network (e.g. on availability or unavailability of the network or the service). A relevant case is that of security breaches, which contribute to the unavailability of a service or of a network component

These metrics are used in both real-time and historically, depending on the organisation. Their increased popularity amongst the stakeholders is mostly due to the relative ease of defining, measuring and combining them. It is a fact that organisations are implementing metrics by starting to use a limited set of simple and well-defined ones.

An open point for discussion is related to the need for combined or complex metrics. While the aggregation or composition of different metrics into only one metric may oversimplify the manner in which possible resilience and security issues are looked at, this provides a useful means of comparison between different networks and services. These higher-level metrics can fulfil several important needs, including those for operational, business and research purposes:

- Troubleshooting for complex, interconnected networks and services

- Means for comparing the performance of different providers

- Supporting capacity planning

- Enhancing improvements and optimisation of networks and services

- Stimulating research and analysis on the evolution of networks and services and suggesting further related metrics.

Linked to the last point above, resilience indicators on the preparedness dimension, such as 'topological robustness' of a network and used capacity, are considered as well, although mostly at design time and not during service operations.

Some of the metrics provided diverge from the accepted understanding of preparedness (being the state of having been made ready or prepared for use or action), and can be even regarded as inappropriate, such as, for example, the strength of the cryptographic technologies used for authentication and encryption. These metrics can be part of design/development targets used during the conception phase of a product or service.

The most cited '**preparedness/design**' resilience indicators are:

- The lifecycle state of the hardware supporting the network (whether or not it is still supported by the equipment vendor) – however, in practice this requires a good view of the asset management database (both hardware and software assets)

- The number of failure points that result in various levels of loss of availability (for example, how many single points of failure result in 50%, 75% or 80% of loss of availability)

- The level of redundancy in the network; published research exists on the theoretical quantification of network element redundancy and network path diversity but, in its current state, it is considered a very conceptual approach and all stakeholders mentioned the practical infeasibility of this metric in large networks

#### 1.1.1.2 Security

By comparison, security is better defined – the traditional terms of confidentiality, integrity and availability are the most commonly used and accepted when describing it. While the term security is readily defined by all stakeholders, it is also far more difficult to measure compared to resilience and therefore there are only a few well-established processes and methods to measure it.

Vulnerability and patch management are mentioned by a few stakeholders as indicators for the security position of an organisation (e.g. the daily vulnerability exposure of a standard workstation). This can be done by comparing the different versions and platforms versus common vulnerability databases such as the MITRE CVE, which can be used as an automated warning system.

Other stakeholders mentioned the regular testing of their Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP); testing the service availability in the face of network challenges (including client infrastructure in the case of service providers) and regular intrusion testing as a way of building trust in the security position within the organisation. Most of these actions do not provide quantifiable results, but still are deemed to be very useful.

#### 1.1.1.3 Data sources

Available and reliable data sources are crucial in the process of defining metrics and executing measurements. Two different types of sources of data are typically used:

- **Active:** based on data from an organisation's own network. Metrics are retrieved, for example, via SNMP and dedicated agents on availability, performance, capacity, etc. In some cases, the measurement process itself is used to generate new events, network traffic, etc.

- **Reactive:** based on data that was accumulated in various repositories, such as the US Vulnerability database, MITRE CVE, the security reports from the different hardware and software vendors, threat levels published on the Internet, such as spam level, Internet threat level, etc.

The data available from the two sources can be used to extrapolate and make predictions about the future. As they are neither objective nor measureable, they should be considered as trends rather than metrics or facts.

Forecasting can be carried out satisfactorily using currently available data to make predictions on future events, but the landscape of the world of network and services changes very rapidly, making a **longer-term prediction** very difficult.

**Short-term predictions** can, however, be made based on statistical intelligence. An example of this is the capacity management of a network, where networks are monitored and, if certain thresholds are exceeded, network expansion is triggered. In the ITIL-framework, this is referred to as 'capacity management' and it is an integral part of the service management processes.

In general, practical difficulties in collecting and analysing data required for the measurements is a very restrictive factor, which impacts the adoption of resilience or security metrics. Many organisations use this argument to challenge the initiatives for defining and using metrics.

**Awareness of specific frameworks, methods and/or tools to measure the effectiveness of policies and controls**
**While most stakeholders are aware of different measurement frameworks, the usage rate of the frameworks remains very low (see Figure 3 and Figure 4).**

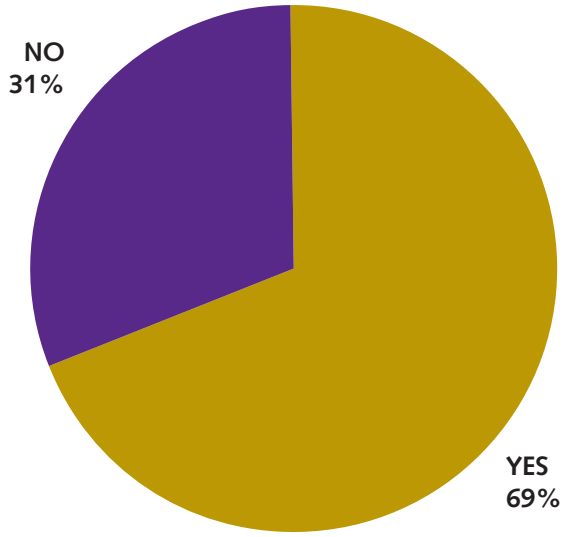



Figure 3: Awareness of specific frameworks, methods and/or tools

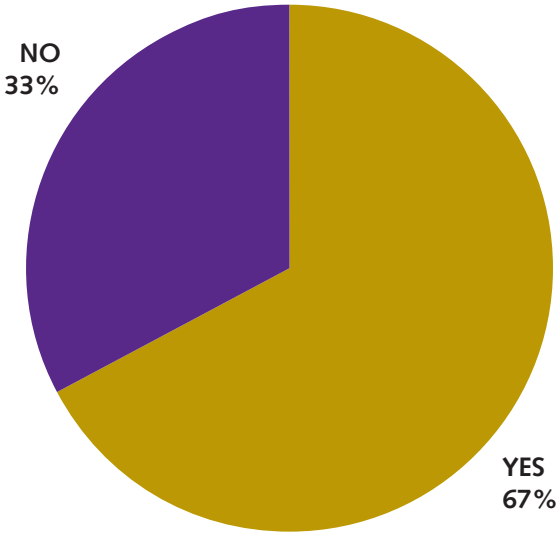



Figure 4: Effective use of specific frameworks, methods and/or tools

### 1.1.1.4 Frameworks

As a general framework with no specific recommendations relating to resilience and security, the Information Technology Infrastructure Library (ITIL)[19] is used by most organisations for guidance in implementing proper management of service quality. A part of the service management framework is dedicated to the management of availability and capacity – the two valuable resilience characteristics mentioned in the previous section.

A control framework, such as COBIT, is mentioned as being used on a large scale by organisations that consider auditing as a measurement technique – especially for the area of security. The number of exceptions noted by these audits is used as a metric in some organisations. However, it is widely acknowledged that frameworks like COBIT do not offer guidance on how to measure, for instance, availability of a service or network – but they do define controls over tools and processes.

Other frameworks referred are ISO/IEC 27001, 27002, 27004, BSI BIP 0074 and the NIST standards on metrics and measurements (as a general explanation of how measurements should be carried out by abstracting from what is to be measured). Every organisation claiming ISO 27001compliance should have a measurement system in place. The ISO 27002 standard dictates a number of controls that can be applied to mitigate the different risks identified in an ISO 27001 system, but does not specify how these risks should be measured and quantified.

When the use of frameworks is not declared, the measurements efforts revolve around:

- Availability
- Business continuity maturity, including service resilience
- Automated tooling for data collection, modelling and visualisation

19 The Information Technology Infrastructure Library (ITIL) is a set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations.

#### 1.1.1.5 Others

Setting the right requirements in the network/service design phase is considered to be a method of ensuring resilience. This can be implemented via a top-down approach, where general resilience policies (set by the risk and/or governance departments) are translated into technical policies and finally into configuration profiles. Supporting tools used are both proprietary and in-house developed, without a particular trend being observed regarding this aspect.

There was an idea of an operator implementing agent-based sensors to measure the intensity of network attacks, as observed by the casual broadband user. The participant admitted that this was a large and complex undertaking and that the organisation had only begun to scratch the surface of the possibilities offered by the extremely large dataset at its disposal.

#### 1.1.1.6 National regulations, recommendations, guidelines and/or administrative provisions related to the adoption or interpretation of security or resilience metrics

In general, there is a low level of awareness of specific regulations or guidelines within the European Member States regarding the adoption of resilience, security metrics or other measurement frameworks.

In some cases, the local regulations require operators to report on the performance quality of their communications networks and on security incidents (but not specifically on resilience). Usually, regulators or other authorities impose and verify the minimum requirements for the provision of publicly available electronic communications services and the security thereof.

Such requirements are usually targeting specific categories of stakeholders – e.g. dominant operators. In several cases, operators are obliged to take all necessary steps to ensure the integrity of the public network services considered (such as telephone and Internet connections) and, in the event of catastrophic network breakdown, or in cases of force majeure, the availability of the public telephone network and publicly available telephone services at fixed locations.

In the UK, Centre for the Protection of National Infrastructure (CPNI) has published a best practices guide for resilience and security[20]. The main recommendation is to take a risk-based approach towards resilience by identifying those applications and services that are deemed mission critical and which carry a high risk to the business if the communication services they depend upon are disrupted. The CPNI guidance is that these services should be decoupled as much as possible from other services and appropriate levels of availability should be foreseen (e.g. by providing redundant routes and routers and foreseeing disaster scenarios).

Other Member States have national guidelines set out by the regulators covering security and availability, but in general these guidelines are not binding.

During the survey, one stakeholder reported the existence of the regulations regarding the financial services industry in his/her country; the local national bank requires oversight of the risk related to the financial systems.

The survey participants agree that services such as cloud computing, which by nature span over multiple countries and geographical areas, must comply with specific regulatory and legal requirements in the countries where they are offered.

It is also clear that, while the section above is about obligations between network service providers and the local regulatory bodies, there is also a binding contract between the network service provider and their clients, which can stipulate a number of obligations, service level agreements and related penalties. Although these are not strict regulations, they do represent a binding agreement.

20 See: http://www.cpni.gov.uk/Docs/resilience-guide.pdf

**Summary of the chapter findings**
In summary, answering questions 1 to 3, the respondents expressed the view that:

- **No standard practices are applied:** it was not possible to point out any standard practices that stakeholders would be using in this area; organisations have their own specific approaches and means of measuring resilience, if they actually have any at all
- **Resilience and security measurements are considered important** but the implementation poses multiple obstacles. **Collection and analysis of the data** are very restrictive factors impacting on the adoption of resilience and security metrics
- **The benefits of resilience metrics are realised and accepted**
- **Availability is believed to be an all-encompassing metric:** downtime, response time and repair time are all considered to be embedded in this metric. Other metrics are less popular
- **The popularity of the metrics** corresponds to the relative ease of defining, measuring and combining them
- Resilience indicators on the preparedness dimension, such as 'topological robustness' of a network and used capacity, are considered as well, although mostly at design time and not during service operations
- Security metrics are considered to be better defined, but far more difficult to measure
- Different data sources allow short-term predictions to be made on some of the metrics
- There is awareness of measurement frameworks, but their usage rate is low
- Setting the right requirements in the network/service design phase is considered as a method of ensuring resilience
- There is a low level of awareness of specific regulations or guidelines

## Measurements

**Categories of metrics**
Most popular metrics and categories of metrics used are described in detail in the ENISA Report on Measurement Frameworks and Metrics for Resilient Networks and Services [2]. In this section of the survey analysis, we include a summary of the most relevant aspects on grouping metrics in categories.

Overall, several types of metrics categories have already been proposed and adopted, depending on the particular area they cover (e.g. security, etc.). In practice, there is little interest in starting to define and use metrics based on the category to which they belong. Grouping metrics in categories is, in general, not a priority.

However, there is acknowledgement that meaningful examples of metrics categories can contribute to a systematic and comprehensive practical approach, when metrics need to be considered, defined and used. Such well defined metrics categories can add real value by ensuring a comprehensive approach towards metrics – all relevant categories would be considered.

An overview of key categories of metrics indicated by the contributors to the survey is summarised in section 0. It continues to indicate an overall low level of maturity and an ad hoc approach in structuring and grouping the metrics used; highlighted is the fact that the (ad hoc) categories used in practice are in no way grouped in line with already defined classifications[21] for metrics.

21 See for example the recommended bibliography in Annexe: [3] [4] etc.

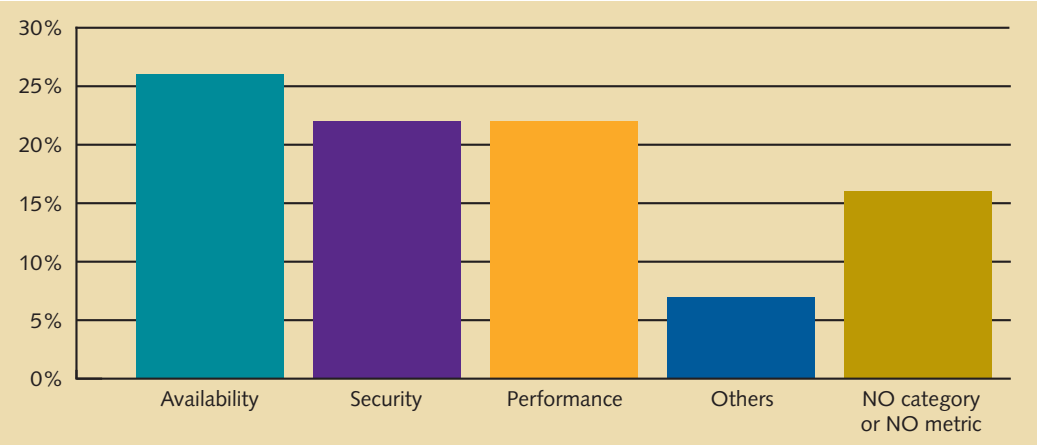



**Figure 5: Key categories of metrics used**

With respect to the frequency of the measurement, there is no clear pattern of the frequency of related measurements based on the metric category.

However, irrespective of the (ad hoc) metric category indicated, there is a more consistent focus and clarity towards the frequency of the metric measurements. The need to adapt the frequency of the measurement to the specific characteristics of the metric is recognised and efforts were made in some cases, for instance, to link it to:

- The level within the organisation at which the user/beneficiary of the metric is positioned, for example: operational, line management, executive. This has a clear influence on the frequency of the measurement:
  - Operational: real-time (continuous), daily and weekly measurements
  - Management: monthly and quarterly measurements
  - Executive: quarterly, semi-annual and annual measurements

- The organisational dimension and/or purpose of the metric, such as whether it is supposed to be technical, operational or organisational

- The requirements:
  - Specific business requirements imposing a particular frequency of measurement;
  - Regulatory requirements that trigger specific reporting needs – for which measurements are necessary
  - Requirements specific to the frameworks, standards, etc. that may have been considered when the metric was defined
  - Some metrics are being gathered only in cases of failures, incidents, unavailability, etc., the measurement being triggered by these events

Although the importance of these items is relatively clear, it is very difficult to establish a relationship between these, the metric category and the specific quantitative measurements.

**Impact**

Resilience metrics are easier to adopt if they are also seen in relation to the impact that is intended to be eliminated. In practice, the impact (e.g. on customers, services, performance etc.) is one of the criteria considered when the usefulness of the metric is analysed.

For example, the manner in which to define and measure availability (or unavailability) can differ dramatically when it is related to the impact on, for example:

- 80% of the customer base, or

- 1% of the customer base

While impact does not actually define the level of resilience of a certain system or service, or the metrics that are used, they are almost always a key element taken into account when the metric is defined and implemented.

**Appropriate thresholds for metrics**
Almost all stakeholders agree that:

- Thresholds are set depending on the designed service (e.g. data versus VoIP)
- Thresholds are related to the Service Level Agreement specifications (availability, recovery time objective, recovery point objective). Thresholds should be relative to a pre-defined baseline and founded on historical measured data in order to be realistic
- There a preference for well-established threshold baselines based on historical data

A few stakeholders suggested determining metrics' thresholds based on the security risks associated with the type of service or system; depending on the probability of the threat and the likelihood of the vulnerability, as well as its potential impact, a decision is made on the thresholds that need to be defined. For example, a threshold such as a certain number of unpatched installations that applies to a router at a customer is not the same as the threshold for a router in the provider's core network (due to the much larger potential impact).

A stakeholder suggested that thresholds should be related to the service provisioning chain and gave the following example: 'If an application needs 99% end-to-end availability (i.e. for the consumer), then the network layer connecting the service provider and the service consumer must offer at least this availability to support the application.'

Some regulators and operators have defined measurement and threshold policies based fundamentally on their own accumulated experience – this is sometimes considered more relevant and appropriate than other external good practices. Others are still in the process of experimenting with metrics and thresholds and have looked into RFC, ANSI and ITU standards to get guidance in defining thresholds. Metrics and thresholds for communications services are generally clearer for the surveyed network operators, compared to security metrics and thresholds.

Different stakeholders mentioned that only reporting the average value of a certain metric is not sufficient for useful interpretation; not only the mean, but also the peak, values of the metric, the median and/or the distribution must be taken into account for the threshold specification. For example:

1. To Voice-over-IP or video applications, the network latency is less critical than the variation of the latency (when the network shows a constant latency, the de-jitter buffers can compensate for that latency. When the latency is not constant, the chances are that the de-jitter buffer either overflows or becomes empty). A quality metric for the latency would be to see the mean latency, the minimum, the maximum and the variance.

2. Another illustration given by the respondents concerned the measurement of a router's processor load. The CPU load of a router is often monitored in large networks. If one would only look at the average load on the CPU, the perception of the load can be false; one could assume that a router is only 70% loaded and thus not overloaded, while in reality the CPU is overloaded during the peak hours of the day and not loaded at all during the night. Therefore, monitoring not only the mean but the minima and maxima as well is very useful.

Many of the stakeholders consider the selection of appropriate metrics and their measurements to be very difficult and acknowledged that defining the thresholds for these metrics is a bridge too far at this point. While selecting appropriate metrics and their measurements is already considered not to be straightforward, determining the right thresholds is even more difficult.

More generally speaking, it is considered a complex undertaking to define the boundaries of the services, due to the incomplete understanding of dependencies and interconnections of those services. When the service is built on the infrastructure of several companies, things can get more complicated.

**Uncertainty when measuring security/resilience metrics**
As a general opinion, the security and resilience metrics are assumed to be meaningful, measurable and correct. Credibility and sufficiency of measured data is also essential.

In this context, it is acknowledged that uncertainty shall be dealt with in a more consistent manner – currently only a few stakeholders are actually considering and dealing with uncertainty when measuring the defined metrics.

Most of these involve:

- Use of probabilistic measures and models
- Measuring and averaging measurements over a long time period (e.g. one year for availability)
- More accurate computation of deviations and errors involved
- Comparisons with similar approaches and results from third parties
- Increased levels of testing and piloting when the metric is implemented
- Identification and filtering of false positives, etc.
- Stronger quantitative / statistical data analysis techniques, such as the distribution, standard deviation and confidence intervals are also used

One recommendation concerning an example framework for uncertainty calculation for security and resilience metrics refers to a framework which calculates the 'trustworthiness of the security measurement', described in the article published in the International Journal on Advances in Security [7].

**Summary of the chapter findings**
In summary, answering questions 4 to 6, the respondents expressed the view that:

- Meaningful examples of category metrics can add to a **systematic and comprehensive practical approach**.
- Still, there is **little interest** in starting to define and **use metrics based on the category** to which they belong
- However, irrespective of the metric category, there is **more consistent focus** and clarity **towards the frequency** of the metric measurements. It is recognised that the **frequency should be adapted** according to the level in the organisation of the beneficiary, the purpose of the metric and the different internal or regulatory requirements
- **Impact** is considered to be a **key element** in evaluating the usefulness of a resilience metric
- **Thresholds** are specific to each service. Preferably, they are based on **historical measurement data**
- Reporting only the average value of a metric is not sufficient for useful interpretation; the peak values, the medium and/or the distribution of the values must be taken into account
- **Uncertainty during measurements** must be **dealt with** in an appropriate way. A number of different approaches have already been identified, ranging from averaging over a longer term to accurate computations of possible deviations

## Analysis and risk management

*Metrics as an iterative tool for security and resilience managers to periodically evaluate the effectiveness of various components*

Using metrics as an iterative tool should be interpreted as the usage of the metrics in the continuous process of repeated evaluations and progressive improvements to the effectiveness of the resilience and security for the different networks, systems and services involved. Effectiveness in this context means the degree to which these systems are considered to be resilient and secure.

When asked about the use of metrics to periodically and recurrently evaluate effectiveness, there is a commonly held view that this is an appropriate manner in which to start, in order to progress towards a set of basic and common areas.

Metrics can be used as a key input in the established process that evaluates and makes gradual improvements:

- Organisations are using the availability metric as a means of checking if redundancy is progressively built into the network. When new systems are being added and/or changed, this could have a negative influence on the availability of a certain service. This would show up in the availability metric and indicate the problem, which will trigger follow-up action. The iterative nature of this lies in the organisational process, which monitors changes in the metric(s) and acts upon them, if necessary.

- Reporting on the number of exceptions noted for the compliance of the different network components or services with the baseline profile is another way to improve resilience or security, in multiple iterations

- Security metrics are generally adopted to periodically evaluate the effectiveness of security programs

- For organisations that have implemented a reporting function: monthly reviews of the relevant metrics report can be a trigger for changes in internal processes/equipment for providing and ensuring a proper level of services, including resilience and security

- The various security metrics and measurements mentioned are also used as input for the risk analysis performed by organisations, usually in the framework of ISO 27001. This is a long-term, gradual process that can benefit from the defined metrics

- Metrics for evaluating the effectiveness of security for the networks and systems involved are sometimes built around the number and type of exceptions or non-compliances noted during frequent penetration tests and security audits. While there is still a debate about whether they are real metrics, they can indicate a trend or change since the last set of penetration tests/audit performed and therefore trigger follow-up actions that will gradually lead to an overall improvement in security

- A regulator indicated that, twice a year, a benchmark report with resilience and security metrics included is sent out to all operators, including the performance of each operator compared to the peer group – this is performed in an anonymised manner and is aimed at improving the overall security and resilience of the networks involved

- When dashboards are developed, they will be more effective in supporting gradual improvements if they include a small set of metrics that speak for themselves. No complex metrics or legacy metrics should be included in a first stage.

**Models, formulas or tools used in the analysis of the measured quantities**
Most stakeholders are not aware of, or are not consistently applying, any existing models, formulas or tools in the analysis of the measured quantities, including combining different metrics, in order to come to more general predictions on the resilience posture and risks in their organisation.

Although models, formulas or tools are used, it is generally acknowledged that they are very difficult to use in order to make predictions on the resilience and security posture of an organisation.

Amongst the most used models are those from operations research and statistics, including (the list is not exhaustive):

- Variance analysis for recognising differences between groups
- Regression models for recognising trends
- Chi square and correlation for understanding interactions and correlation
- Cluster analysis
- Principal component analysis
- Time series analysis
- Reliability growth analysis
- Queuing models
- Various heuristic models

Several operators reported using a combination of in-house developed and open source tools to gather information and to process it, based on a variety of models and defined formulas, none of which is generally accepted and standardised. The processed information is further summarised in a well-defined dashboard, which is usually focused on either security or on resilience, and is not linked to risk aspects. In general, resilience and risks are not jointly dealt with in organisations.

**Summary of the chapter findings**
In summary, answering questions 7 and 8, the respondents expressed the view that:

- Metrics are deemed **useful as an iterative tool**. Their implementation should be a **continuous process of repeated evaluations of and progressive improvements** to the effectiveness of the resilience and security for the different networks, systems and services involved
- The **various security metrics** are also used as input for the risk analysis performed by organisations
- Most stakeholders are **not aware of**, or are **not consistently applying, existing formulas** or models in the analysis of the measurements

## Collaboration and information exchange

*Initiatives between authorities, private sector, academia, or other stakeholders to align efforts regarding security or resilience metrics*

In general, there is increased awareness of the ongoing initiatives to align efforts regarding security and resilience metrics. However, these are usually ad hoc and take place at national level (very few pan-European or cross-border examples were highlighted). Both public and private stakeholders are amongst initiators. A good level of collaboration is reported, for example, in the UK EC-RRG (Electronic Communication Resilience and Response Group[22]).

22 EC-RRG aims to promote the availability of electronic communications infrastructure for the UK and provide an industry emergency response capability. See also: http://www.cabinetoffice.gov.uk/ukresilience.aspx

A large number of respondents from the academic world indicated that such alignment initiatives are considered very useful and that they should be the subject of a national programme of action involving national authorities, **academia**, industry and other key stakeholders. However, it is still generally unclear who should initiate or facilitate such programme.

However, among the stakeholders from the **industry** there is still insufficient awareness of the potential benefits of alignment initiatives regarding the use of security or resilience metrics. A positive/success factor may be getting adequate involvement and support from key industry representatives (e.g. major operators, or those involved in standardisation).

Alignment initiatives are only now just starting and resilience is still low on the agenda of those responsible for these initiatives, in comparison with security. The metrics themselves and were not an active topic in the previous years. One particular opinion presented indicates that the benefits of aligning security metrics are more obvious, while it is still unclear what the corresponding benefits of sharing resilience metrics are. This is an obvious indication that increasing awareness on the benefits should become a priority.

**Exchange of information with authorities or other stakeholders (e.g. CERTs) on security or resilience metrics**
The majority of participants were aware of information exchange initiatives, usually facilitated by national (where they exist) or industry CERTs. However, only half of all participants were actually active in such initiatives (see Figure 6). Information exchange is also accomplished via participation in relevant industry and public bodies.

The participation in information exchange on security or resilience metrics does not indicate any specific pattern related to the type of organisation involved.

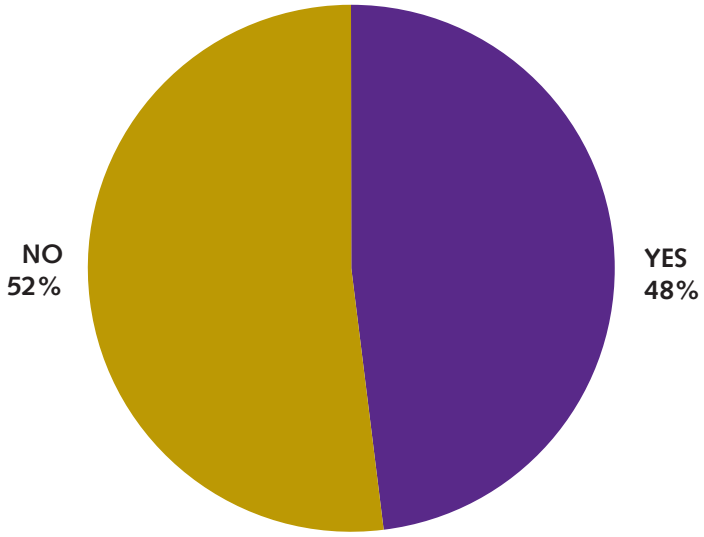



**Figure 6: Involvement in information exchange**

In certain cases, information is exchanged and particular topics are discussed as part of an established national legal framework, also with the intention of establishing contacts and improving mutual awareness. Involved actors may, for instance, primarily create and share metrics based upon public data sources (e.g. US NIST National Vulnerabilities Database, the Open Security Foundation's Dataloss DB, and others) and work with owners of private multi-company datasets to produce analysis that can be shared and published without exposing individual organisations.

In the case of CERT-facilitated information exchanges, one of the recognised challenges is to combine CERT information with that coming, for instance, from telecom operators – due to different information sharing cultures.

Fully detailed **resilience** metrics are generally not shared; however the key measurements of network or service availability and some other indicators related to resilience are often published[23] and exchanged with other stakeholders.

Almost all stakeholders confirmed that information sharing, especially in regard to security metrics, is avoided by organisations. This is due to the concern that sharing information on incidents could decrease the consumer / peer group trust and might also give attackers more information about security practices, rendering the organisation an easy target for cyber security attacks.

A driver for participating in information exchange is the willingness to contribute in a community and to share/publish data for the purposes of defining and refining metrics, as well as for understanding where organisations stand as compared with peers (e.g. same industry or specific). It is expected that information exchange takes place in a 'trusted environment' that would allow contributors to learn from each other and work together to solve a specific problem related to resilience or security.

There is an indication of an increased desire to exchange information on security or resilience metrics across industries. Currently, many such initiatives are within the same industry, in some cases being limited to one-to-one discussions. Organisations should be encouraged and even incentivised to be transparent and share from the lessons learned from their own efforts in adopting and implementing metrics for resilience and security. They should undertake a more active role and pro-actively consider publishing, as good practice, the most relevant adopted metrics and also narrative that provides interpretation and rationale.

**Summary of the chapter findings**
In summary, answering questions 9 and 10, the respondents expressed the view that:

- **Alignment initiatives are just starting now** and resilience is still low on the agenda of these initiatives
- There is an **increased awareness of the ongoing initiatives** to align efforts regarding security and resilience metrics
- There are a large number of respondents in the academic world that consider **alignment initiatives very useful** – although it is unclear who should initiate such a programme
- The majority of the **information exchange initiatives** are facilitated by national or industry **CERTs**
- **Regarding information sharing barriers:** a recognised limitation in applying resilience measurement frameworks and metrics has its root causes in the relatively limited information exchange on current good practices. Some **categories of organisations have a strong culture** and a tendency to avoid transparency and they protect the information on their level of maturity and expertise in this area. In many cases, they are simply declining to comment on security and resilience postures and practices

## Problems and suggestions

*Technical or other factors that hinder the application of security/resilience measurement or assessment methods*

### 1.1.1.7 Technical limitations

Although most stakeholders are actively measuring the resilience and/or security of their networks and services - albeit by using availability as a general metric - they confirm that no readily available tools/solutions for measuring resilience and security exist. This is one of the most relevant (technical) limitations disclosed.

23 For example on: www.metricscenter.net

Outdated in-house developed tools, or insufficient budget for acquiring or developing adequate new ones, was also systematically indicated as a blocking factor.

The cost of data gathering, data modelling and processing/analysis is a limiting factor as well, especially given the vagueness of the metrics to be used and the changes in the measurement methodologies used.

Common obstacles identified with regard to data gathering and processing/analysis are:

- Insufficient data volume can be collected to allow good trend analysis
- No interoperability of the different analysis results (which leads to comparing result categories that are not correlated)
- Benchmarks not detailed enough (for example, by not making a distinction between critical and non-critical services)

There are some ongoing concerns related to the risk of putting high loads on the networks or services in the case of continuous or real-time measurements. This is a major limitation noted in the case of telecommunication operators, ISPs, etc. and leads to reluctance and excessive caution when adopting metrics.

In practice, it may also affect the relevance of the measurement and generate errors. For example, continuous polling of the traffic flows on a router drains the processing resources of that router and will have a significant impact on the amount of traffic that the router can handle per unit of time.

### 1.1.1.8 Other limitations

Availability of data and of insights into the adopted metrics (best practices) is another important limitation – due in this instance to the lack of trust between the organisations and their reluctance to share sensitive security data. The quote below is very relevant in this context:

*'The primary barrier to benchmarking can be called a 'Tragedy of the Anti-Commons'. Owners of data are exercising their right NOT to share to the (tragic) detriment of the common good. The reason for not sharing is fear of exposure. One way to address this is through anonymous submission of data, which is technically possible.'*
**Quote from a security services provider**

There is no general consensus on definitions, measurement frameworks and good practice guides that can help and accelerate the implementation of resilience and security metrics. This usually undermines the early stage initiatives of those involved and responsible for promoting adoption of resilience and security metrics and in getting priority for this within their own organisation.

Additionally, some metrics such as Mean Time Between Failures are very theoretical when applied to network systems (due to the complexity of and many interdependencies in those systems) or are not supported by generally accepted methods of measurement and are therefore difficult to put into practice.

From an organisational viewpoint, there are in practice cases where there are two (or more) separate functions responsible for resilience and security respectively. This creates additional obstacles, due to internal misalignments, different approaches, lack of focus and separate sets of metrics or different frameworks used. This happens mostly due to the fact that security and network engineering are positioned as different sections within the same organisation.

**Advice to organisations starting out to design and implement a metric scheme**
Definitions of the metrics to be used depend on specific business requirements – there is an obvious agreement on this. Moreover, some network operators and ISPs specifically insist that this shall be the key driver in considering, defining and using metrics – a valid viewpoint from an industry perspective. The business requirements will not only dictate the different metrics to be used, but also the thresholds that should be associated with them – this is an aspect that requires further consideration.

These requirements can be deduced from internal or external Service Level Agreements (SLAs), including the assessment of impact – there is a major difference between a temporary SLA violation for a few users and for the entire client base, or from regulatory agreements, if applicable. An additional step can be to apply an 'impact factor' to the different services, to indicate that not all threshold violations are equally severe and/or likely.

There were many viewpoints expressed that favoured the idea that an organisation starting a measuring process should first implement a limited set of metrics to avoid implementations that were too complex and lengthy. This would also facilitate the internal buy-in from the various levels within the organisation towards the implementation of metrics.

In the initial measurement phase, the different measurements should be used to establish a reference value, effectively an 'expected' value, considered to reflect the normal state of operations for the system or service. This value should be accompanied by an acceptable range for the measurement and would be the basis for setting thresholds later on.

A few stakeholders feel that the national regulator should more actively give guidance on resilience and security standards and measurement methods for the different operators. The other stakeholders involved should actively seek for guidance on this topic from the national regulators.

**Key unsolved problems in assessing, measuring, and benchmarking the security and resilience of networks and services**
The lack of consensus and lack of standardised and generally accepted metrics and measurement frameworks is agreed to be one of the major drawbacks. This issue was highlighted over and over again and obviously needs further efforts from all interested parties in order to be resolved. The solution may be increased collaboration in different forums and formats between three key categories of stakeholders involved: academia, the industry and the regulators.

*'Currently, security and resilience of communication networks and services are driven by the market. It is the general perception that objectives regarding security and resilience have been (already) achieved without defining formal criteria. Therefore, it will be hard to achieve improvements by defining such criteria and to justify the cost-benefit ratio...'*
**Quote from a regulator**

Not only is the lack of tools a factor that makes the measurement of resilience difficult, but also the lack of knowledge and information exchange on this topic. Continuous investment is recommended in order to build and broaden the necessary knowledge level and to allow involved professionals to be up to date with the research, technical and regulatory developments and trends that may impact on this domain.

It is suggested that too much emphasis is currently placed on measuring and providing countermeasures, while the link to the risks involved is often forgotten or neglected. Beginning from a risk perspective would help to move the focus towards the right metrics and tools required to retrieve those measurements. The quote below is relevant in this context:

*'In my opinion, resilience is not a particularly mature area in relation to other areas of business risk. In terms of countermeasures, I think resilience is quite well understood; but the countermeasures often stop at the network, rather than being sensitive to the services that run across them. ... I would concentrate on developing a metric framework for resilience and to map the countermeasures to the areas identified as high impact and high risk.'*
**Quote from a regulator**

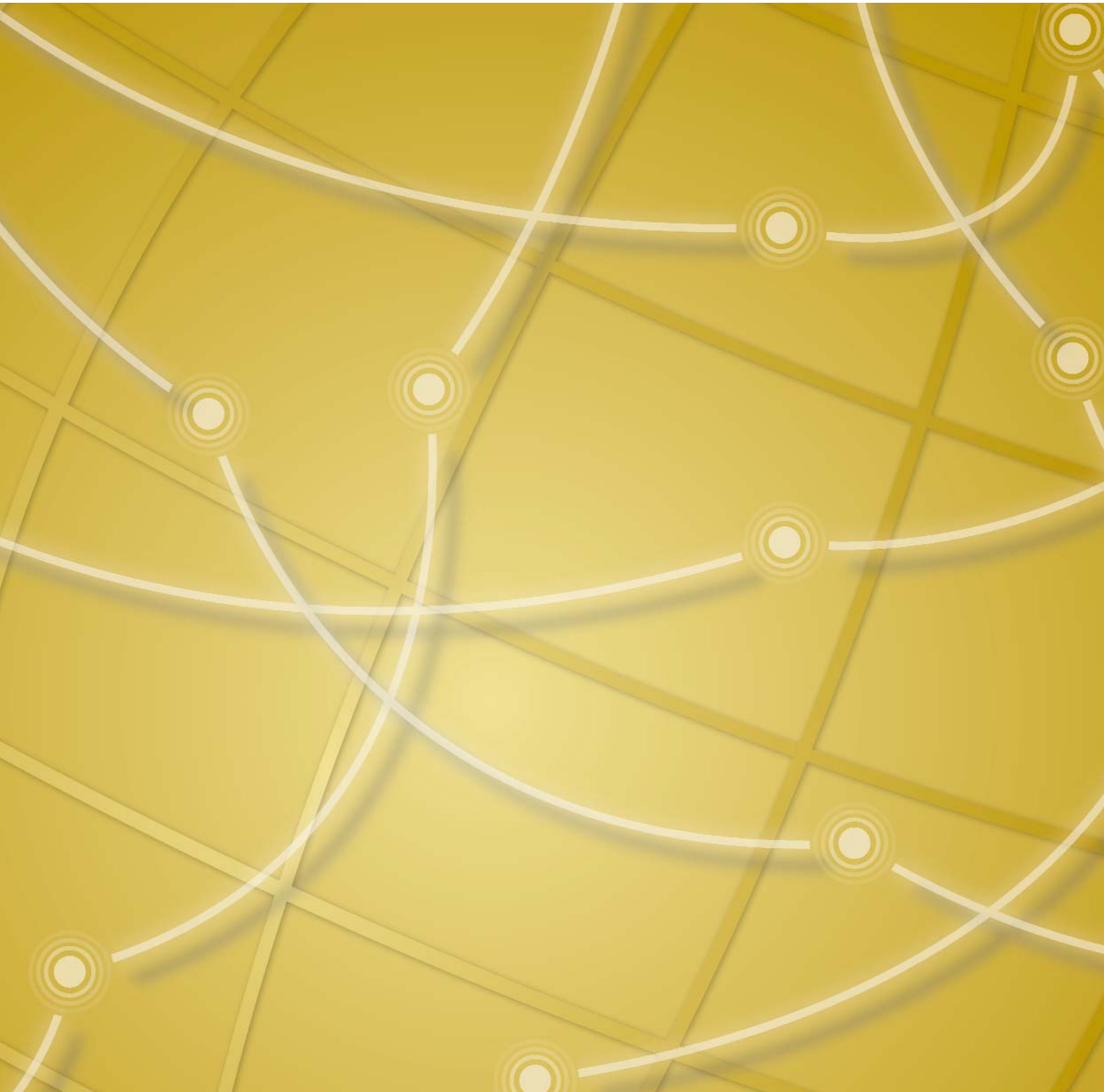
**Summary of the main findings**
In summary, answering questions 11 to 13, the respondents expressed the view that:

- A number of **technical limitations:**
  - Although most stakeholders are actively measuring the resilience and/or security of their networks and services - albeit by using availability as a general metric - all stakeholders confirm that no **readily available tools/solutions for measuring resilience and security exist**
  - **Cost of data gathering** is a limiting factor
  - **Limitation** on the data analysis possibilities

- **Other limitations**
  - **No consensus** on definitions and **good practice and lack of standardised and generally accepted metrics** and measurement framework undermines early stage implementations
  - The **existence of organisational walls** between those responsible for resilience and security, impeding efficient communications

- **The main advice** is to base the resilience and security metrics on **existing business requirements** and to start out with a **small set of metrics**, which gradually expands. During this initial phase, **reference values** should be defined that will reflect the 'normal state of operations'. Using these reference values, metric benchmarking and **thresholds** become possible.

# Annexes



# Annexe A - Methodology used

The study and its associated survey adopted a three-stage approach for the collection of detailed information, as graphically depicted in Figure 7.

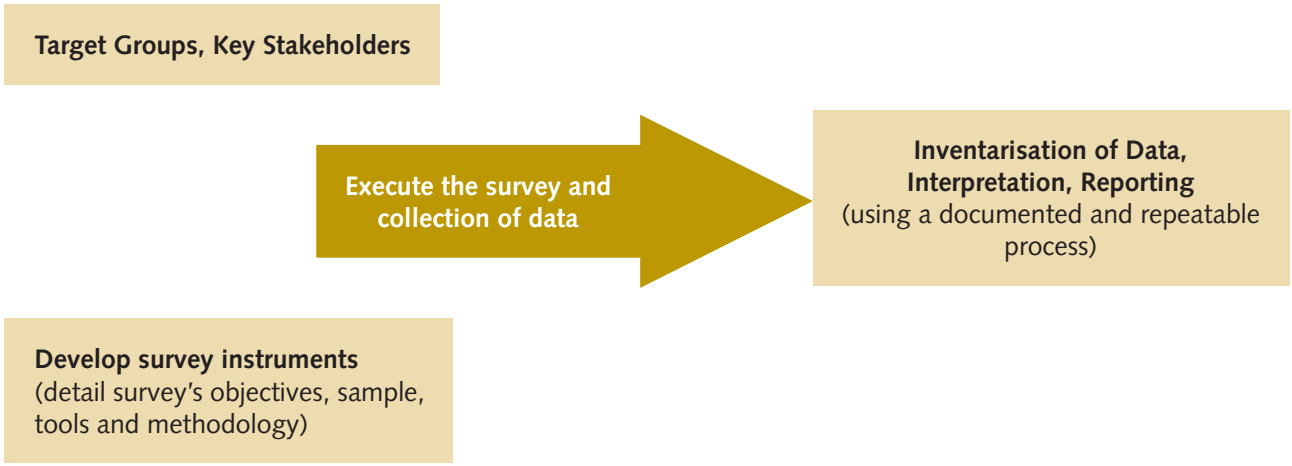



**Figure 7: Stakeholder survey approach**

After the collection of the survey responses, the areas of consensus, as well as points of divergence, were identified. As agreed with the interviewees and in compliance with Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000, all interviews have been treated in confidence and the results are not attributed to individual persons.

Subsequently, a workshop will validate the results of the analysis and the recommendations for a good practice list with the stakeholders.

# Annexe B - Survey questions

The questions below were sent to the different stakeholders:

| Topic | Question |
|---|---|
| **Strategy and governance** | 1. How do you measure the resilience and security of communications networks and services?<br>2. Do you use or are you aware of any specific frameworks, methods and/or tools that measure the effectiveness of policies and controls related to resilience and security of communications networks and services?<br>3. Are there any regulations, recommendations, guidelines and/or administrative provisions in force in your country related to the adoption or interpretation of security or resilience metrics for networks and services? Which areas do they cover? |
| **Measurement** | 4. Which categories of metrics are or should be measured and reviewed within an (your) organisation? How and how often do you measure metrics for each category?<br>5. How do you establish the appropriate thresholds for each metric?<br>6. Do you evaluate uncertainty when measuring security/resilience metrics? How? Which countermeasures do you adopt to reduce measurement uncertainty? |
| **Analysis and Risk Management** | 7. To what extent and how are metrics adopted as an iterative tool for security and resilience managers to periodically evaluate the effectiveness of various components of their security programs, system, product or process?<br>8. Are there any models, formulas or tools used in the analysis of the measured quantities, including combining different metrics, in order to come to more general predictions on the resilience posture and risks in your organisation? |
| **Collaboration and Information Exchange** | 9. Are you aware of any initiatives between authorities, private sector, academia, or other stakeholders in your country to align efforts regarding security or resilience metrics and/or benchmark their results and trends? How do you believe something like this would be helpful?<br>10. Do you exchange information with authorities or other stakeholders (e.g. CERTs) on security or resilience metrics? Could you clarify what information is exchanged exactly and how this could be further enhanced? |
| **Problems and Suggestions?** | 11. Could you identify technical or other factors that hinder the application of security/resilience measurement or assessment methods? (e.g., lack of tools, lack of benchmarks and information exchange, lack of interfaces to collect security/resilience data)<br>12. What advice would you give to organisations starting out to design and implement a metric scheme in terms of practical approach? Are there particular good practices you recommend to be considered or risks to be taken into account?<br>13. In your opinion, what are the key unsolved problems in assessing, measuring, and benchmarking the security and resilience of networks and services? What are the main research challenges we need to tackle in the near future that should be considered when developing a good practice guide? |

# Annexe C - List of respondents / contributors

We would like to acknowledge the contribution of the following participants in this survey and to thank them for the valuable input and viewpoints provided.

| | |
|---|---|
| AGH University of Science and Technology | **Andrzej Jajszczyk** |
| AGH University of Science and Technology | **Piotr Cholda** |
| ANCOM – The Romanian Regulatory Authority | **Catalin Marinescu** |
| ANISP – The National Association of ISPs from Romania | **Gheorghe Serban** |
| AT EZ | **Eelco Vriezekolk** |
| Azercell | **Orhan Buday** |
| Certipost | **Jan D'Herdt** |
| Comreg | **Paul Conway** |
| CPNI | **Andrew Powell** |
| Deutsche Telekom | **Joachim Hoenig** |
| Deutsche Telekom | **Thomas Tscherisch** |
| EETT - Hellenic Telecommunications and Post Commission | **Sofia Fragkoulopoulou** |
| ENEA | **Gregorio D'Agostino** |
| ETSI | **Carmine Rizzo** |
| Eurocontrol | **Jean-Louis Tastenhoye** |
| European Defence Agency | **Thomas Lenschen** |
| Euroweb | **Gheorghe Covrig** |
| FICORA | **Pertti Hölttä** |
| Geant / Dante | **Dai Davis** |
| Hochschule Luzern HSLU / Acris GmbH | **Prof. Bernhard M. Haemmerli** |
| Idaho National Laboratory | **Wayne Boyer** |
| Interoute | **Joe Stevens** |
| ISACA | **Rastislav Machel** |
| ISACA / Deloitte | **Fadi Mutlak** |
| ISACA / KPMG | **Rolf von Rössing** |
| ISO - SC27 | **Edward Humprhreys** |
| IT-ISAC | **Scott C. Algeier** |
| Kasperski | **Mirco Rohr** |
| KPN | **John van Leeuwen** |
| Microsoft | **Matt Broda** |

| | |
|---|---|
| NIST | **Anoop Singhal** |
| Nokia | **Erkki Kataja** |
| Norwegian Post and Telecommunications Authority | **Håkon Styri** |
| OFCOM / Swiss Confederation | **Mark Fitzpatrick** |
| Plexlogic | **Elisabeth Nichols** |
| PTS Swedish Post and Telecom Agency | **Anders Johanson** |
| RTR / Austrian Regulatory Authority for Broadcasting and Telecommunications | **Ulrich Latzenhofer** |
| s21Sec | **David Barroso** |
| SWIFT | **Herwig Thyssens** |
| TMIT Budapest University of Technology and Economics | **Tapolcai Janos** |
| TNO | **Robert Kooij** |
| University Gent | **Mario Pickavet** |
| University of Lancaster | **David Hutchison** |
| University of Ljubljana FDV | **Denis Trcek** |
| University of Naples Federico II | **Leopoldo Angrisani** |
| Vodafone Albania | **Yiannis Theodorakos** |
| Vodafone Italy | **Corradino Corradi** |
| VTT Technical Research Centre of Finland | **Reijo Savola** |
| Yandex | **Kupriyanov Alexander** |

# Annexe D - Other sources recommended

During the interviews and in the survey responses received, the contributors made reference to a number of relevant information sources that can provide help and valuable information in defining, analysing and adopting measurement frameworks and metrics for resilient networks and services.

We list below a selection of these recommended sources – the list is not exhaustive:

**[1]** Measuring Cyber Security and Information Assurance, State-of-the-Art Report (SOAR), 2009, by Information Assurance Technology Analysis Center (IATAC);

**[2]** ENISA Report on Measurement Frameworks and Metrics for Resilient Networks and Services;

**[3]** Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy, Department of Computer Science Mississippi State University, 2002;

**[4]** Process Control System Security Metrics – State of Practice', I3P – Institute for Information Infrastructure Protection, 2005;

**[5]** Framework for resilience developed within the ResiliNets initiative (see also https://wiki.ittc.ku.edu/resilinets/Main_Page), which is a joint activity between the Universities of Kansas and Lancaster;

**[6]** D. Trček, Managing Information Systems Security and Privacy, Springer, 2006, Heidelberg / New York, page 16;

**[7]** Reijo Savola - VTT Technical Research Centre of Finland, Oulu, Finland; Habtamu Abie - Norwegian Computing Center, Oslo, Norway; Development of Measurable Security for a Distributed Messaging System; International Journal on Advances in Security

**[8]** Boyer, W.F., McQueen, M.A., 'Ideal Based Cyber Security Technical Metrics for Control Systems', CRITIS'07 2nd International Workshop on Critical Information Infrastructures Security, October 3-5, 2007, LNCS 5141,
pp. 246-260, 2008;

**[9]** J.P.G. Sterbenz, D. Hutchison, E.G. Cetinkaya, A. Jabbar, J.P. Rohrer, M. Schöller, and P. Smith, 'Resilience and survivability in communication networks: strategies, principles, and survey of disciplines', Computer Networks - Special Issue on Resilient and Survivable Networks, Elsevier, Vol. 54, N° 8, June 2010, pp. 1245-1265;

**[10]** L.Angrisani, M.Vadursi, 'Cross-Layer measurements for a comprehensive characterization of wireless networks in the presence of interference', IEEE Trans. on Instr. and Meas., vol.56, No.4, Aug. 2007, pp.1148 - 1156;

**[11]** David A. Chapin and Steven Akridge. 'How Can Security be Measured?' in ISACA Information Systems Control Journal, Volume 2, 2005.

**[12]** L.Angrisani, A.Pescapè, M.Vadursi, G.Ventre, 'Performance measurement of IEEE 802.11b-based networks affected by narrowband interference through cross-layer measurements', IET Communications, vol.2, No.1, Jan. 2008, pp.82 91;

**[13]** L.Angrisani, M.Farias, D.Fortin, A.Sona, 'Experimental analysis of in-channel interference effects on the performance of a DVB-T system', IEEE Trans. on Instr. and Meas. vol.58, No.8, Aug. 2009, pp.2588 2596;

**[14]** L.Angrisani, A.Napolitano, A.Sona, 'Cross-layer measurements on an IEEE 802.11g wireless network supporting MPEG-2 video streaming applications in the presence of interference', EURASIP Journal on Wireless Communications and Networking, Hindawi Publishing Corporation, vol.2010, Article ID 620832, Apr. 2010, pp.1-11;

**[15]** John I. Alger, on Assurance, Measures, and Metrics: 'Definitions and Approaches, in Proceedings of the Workshop on Information Security System Scoring and Ranking Information System Security Attribute Quantification or Ordering (commonly but improperly known as Security Metrics)', Williamsburg, Virginia, 21-23 May 2001 (commonly referred to as the Workshop on Information Security System Scoring and Ranking [WISSRR]);

**[16]** P. Chołda, J. Tapolcai, T. Cinkler, K. Wajda, A. Jajszczyk, 'Quality of Resilience as a Network Reliability Characterization Tool', IEEE Network, vol. 23, no. 2, March/April 2009, pp. 11-19;

**[17]** P. Chołda, A. Jajszczyk, K. Wajda, 'A Unified Quality of Recovery (QoR) Measure'; International Journal of Communication Systems (Wiley), vol. 21, no. 5, May 2008, pp. 525-548;

**[18]** P. Chołda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner, A. Jajszczyk, 'A Survey of Resilience Differentiation Frameworks in Communication Networks', IEEE Communications Surveys and Tutorials, vol. 9, no. 4, 2007, pp. 32-55;

**[19]** P. Chołda, A. Jajszczyk, 'Recovery and its Quality in Multilayer Networks,' IEEE/OSA Journal of Lightwave Technology, vol. 28, no. 4, February 15, 2010, pp. 372-389;

**[20]** P. Chołda, A. Mykkeltveit, B. E. Helvik, and A. Jajszczyk, 'Continuity-based Resilient Communication' 7th International Workshop on the Design of Reliable Communication Networks DRCN 2009, Washington, D.C., USA, October 25-28, 2009;

**[21]** Victor-Valeriu Patriciu, Iustin Priescu and Sebastian Nicolaescu. 'Security Metrics for Enterprise Information Systems' in Journal of Applied Quantitative Methods (JAQM), Vol. 1, No. 2, Winter 2006;

**[22]** John P. Pironti. 'Developing Metrics for Effective Information Security Governance,' ISACA Information Systems Control Journal, Volume 2, 2007;

**[23]** Khalid Kark and Paul Stamp, Forrester Research. 'Defining an Effective Security Metrics Program' 16 May 2007.


PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
**www.enisa.europa.eu**