TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA Cybersecurity Market Analysis Framework (ECSMAF) – V3.0

A framework for market analysis, including market monitoring, in the cybersecurity domain

MARCH 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, use market@enisa.europa.eu.
For media enquiries about this paper, use press@enisa.europa.eu.

AUTHORS (IN ALPHABETICAL ORDER)

Nico Abbatemarco, Università Bocconi
Benedetta Burston, Università Bocconi
Louis Marinos, ENISA
Greta Nasi, Università Bocconi
Silvia Portesi, ENISA

ACKNOWLEDGEMENTS

We would like to thank the ENISA National Liaison Officers, the ENISA Advisory Group members, Carmelo Dimauro (National Cybersecurity Competence Center Luxembourg (NC3)), Bertrand Lathoud (University of Luxembourg), Riccardo Zecchinelli (National Cybersecurity Agency (ACN), Italy), and the ENISA colleagues, who reviewed drafts of this deliverable and provided their feedback.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.
ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and must be accessible free of charge. All references to it or its use as a whole or in part must contain ENISA as its source.
Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-780-1, doi:10.2824/4565747, Catalogue Number: TP-01-25-035-EN-N

Table of Contents

Executive Summary

The European cybersecurity market is rapidly evolving, shaped by new legislative requirements such as the Cyber Resilience Act (CRA), the growing relevance of products with digital elements and an increasing demand for timely and structured market intelligence.

To address these developments, the European Union Agency for Cybersecurity (ENISA) has updated its cybersecurity market analysis framework, first published in 2022 and revised in 2023.

Under Article 8(7) of the Cybersecurity Act, ENISA is mandated to 'perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union'.

This new version of the ENISA Cybersecurity Market Analysis Framework (ECSMAF) (Version 3.0) incorporates lessons learned from previous applications and strengthens the framework's ability to respond to both immediate policy needs and long-term monitoring requirements. The updated framework makes cybersecurity market analyses:

- **more responsive to constraints**, by allowing analyses to be conducted within tight delivery windows while maintaining quality, thanks to standardised templates, simplified data collection methods and reusable materials;
- **more data driven and efficient**, by promoting the use of modular tools, reusable taxonomies and stakeholder-specific question sets to streamline processes and reduce duplication;
- **more flexible in their workflows**, by offering configurable pathways that adapt to the scope, timing and depth of analysis, whether for fast-tracked ad hoc requests or comprehensive planned studies;
- **more sustainable over time**, by enabling recurrent market analysis and continuous monitoring of market dynamics, and comparability across studies, and supporting cumulative insight into European cybersecurity developments;
- **more attuned to recent regulatory developments**, by aligning analytical pathways with regulatory priorities and ensuring that categories of high policy relevance are systematically captured and assessed.

The framework comprises seven steps to guide analysts in conducting a cybersecurity market analysis:

- Step 1 – Initiate the analysis;
- Step 2 – Scope the market segment for analysis;
- Step 3 – Analyse the market segment;
- Step 4 – Describe the 'what' and the 'how';
- Step 5 – Collect the data;
- Step 6 – Analyse the data;
- Step 7 – Present and disseminate the results.

Depending on stakeholders' needs, ECSMAF Version 3.0 may be used for market analyses of a very short / short (taking less than six months) or long duration (taking more than six months), but also for recurrent analyses or continuous monitoring.

ECSMAF has been developed with reference to ENISA's mandate and the needs of its stakeholders. However, the structure and logic of the framework are sufficiently generic to allow its application, with limited customisation, by organisations other than ENISA.

1. Introduction

1.1 Aims of This Framework

This framework is a guide on how to conduct market analysis, including recurrent market analysis and continuous market monitoring, in the field of cybersecurity. It aims to:

- provide a methodology for analysing and documenting cybersecurity market segments;
- enhance rigour and structure in analysing the market, on both the demand and the supply side, of (new) cybersecurity products, services and processes;
- enable the better analysis and understanding of cybersecurity trends on both the supply and the demand side;
- inform policy decisions with robust market data, by providing evidence-based and structured market insights;
- identify emerging fields and investment opportunities in the cybersecurity domain;
- promote the EU's cybersecurity market by assessing its needs in terms of certification, market surveillance, dependencies, strengths and weaknesses, etc.;
- facilitate decision-making based on comparable data and knowledge transfer.

1.2 Target Audience

The framework has been developed to address the needs of the European Union Agency for Cybersecurity (ENISA) and its stakeholders with regard to cybersecurity market analysis.

The framework serves analysts across EU institutions, bodies and agencies, national authorities and industry associations, along with consumer and research organisations, companies on both the supply and the demand side of cybersecurity, and venture capitalists seeking to understand market opportunities.

While designed primarily for public-sector stakeholders and strategic analysts, private companies (both on the supply and the demand side) may find the framework useful for market scoping, along with procurement and investment planning.

1.3 Background and Policy Context

ENISA initiated its work in the area of cybersecurity market analysis in 2021 as part of its task to 'perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union', as set out in Article 8(7) of the Cybersecurity Act (CSA) ([1]) and as mentioned in Recital 42 of the CSA.

As part of this work, ENISA has developed the ENISA Cybersecurity Market Analysis Framework (ECSMAF), on which basis it performs its market analyses. The first version of this framework,

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj) (accessed 22/07/2025).

ECSMAF Version (V) 1.0, was published in 2022 [2], while a second one, ECSMAF V2.0 [3], was released in 2023.

The framework has so far been applied to a series of market analysis studies, including ENISA's market analyses of cloud cybersecurity [4], cryptographic products and services [5] and managed security services [6]. The current version of the framework, ECSMAF V3.0, incorporates lessons learned from previous market analyses, such as the need to conduct market analyses in a more reactive and timely manner, and to allow for scalability. The application of ECSMAF V2.0 highlighted the need to update the framework with a focus on improving aspects related to, for example, timeliness, frequency, data collection and suitability for sustained and long-term market monitoring (instead of one-off market reports) to enable the delivery, in a timely manner, of regular and ad hoc market analysis reports for use in market monitoring.

Moreover, ECSMAF needed to be aligned with recent legislative initiatives, such as the Cyber Resilience Act (CRA) [7], establishing cybersecurity requirements for digital products, and the Network and Information Systems (NIS) 2 Directive [8], enhancing resilience across critical infrastructures.

1.4 What is New in This Version of the Framework

The present ECSMAF aims to better fit ENISA's and its stakeholders' specific objectives.

Moreover, ECSMAF V3.0 builds on the previous versions of the framework, offering a more streamlined, user-friendly approach (e.g. by introducing reusable templates), with continuous change expected in future updates.

Finally, ECSMAF V3.0 supports recurrent analysis and continuous monitoring (see the section 'One-off and Recurrent Market Analysis and Continuous Market Monitoring'), enabling periodic updates as well as continuous observation on the same market segment as conditions evolve.

1.5 Initiation and Duration: Two Core Pillars of the Framework

Two important pillars of ECSMAF V3.0 are:

- the **initiation of the analysis** (whether it is planned internally or initiated in response to an ad hoc request);
- the **duration** (in other words the time constraints) of the analysis (short or long duration).

These two pillars determine the configuration of the analysis and guide the selection of methods, tools and engagement strategies at each step of the workflow. This dual structuring

[2] ENISA, *ENISA Cybersecurity Market Analysis Framework (ECSMAF)*, 2025, https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf (accessed 22/07/2025).

[3] ENISA, *ENISA Cybersecurity Market Analysis Framework (ECSMAF) V2.0*, 2023, https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0 (accessed 22/07/2025).

[4] ENISA, *Cloud Cybersecurity Market Analysis*, 2023, https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis (accessed October 2025).

[5] ENISA, *Cryptographic Products and Services Market Analysis*, 2024, https://www.enisa.europa.eu/publications/cryptographic-products-and-services-market-analysis (accessed 22/07/2025).

[6] ENISA, *MSS Market Analysis – An analysis of the managed security service market*, Publications Office of the European Union, Luxembourg, 2025, https://www.enisa.europa.eu/publications/managed-security-services-market-analysis (accessed 22/07/2025).

[7] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj) (accessed 22/05/2025).

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj) (accessed 22/07/2025).

ensures that the framework remains both flexible and fit for purpose, accommodating a variety of analytical scenarios and resource conditions.

There are two reasons for **initiating** an analysis.

- **Planned analysis.** A comprehensive market study can be initiated as part of ENISA's strategic planning process (e.g. when implementing ENISA's single programming document). It supports forward-looking priorities and contributes to ENISA's long-term objectives. Planned analyses may be short or long in duration as a result of time constraints, depending on the depth of exploration and the methodological requirements.
- **Analysis following an ad hoc request (also referred to as 'ad hoc analysis').** An analysis can be conducted to address a specific request (e.g. from the European Commission or from an EU Member State, or driven by cybersecurity events such as recurring incidents in particular market segments), typically resulting from immediate policy needs, strategic developments, situational awareness, etc. The scope and methodology are defined based on the nature of the request and available resources. Ad hoc analyses may be short or long in duration.

The **duration** of analysis can be:

- **less than six months** (short with the possibility of being very short), which means that the time available for performing the analysis is tight and therefore an accelerated method is needed;
- **more than six months** (long with the possibility of being very long).

Depending on the context of initiation and duration, different analysis pathways are applied.

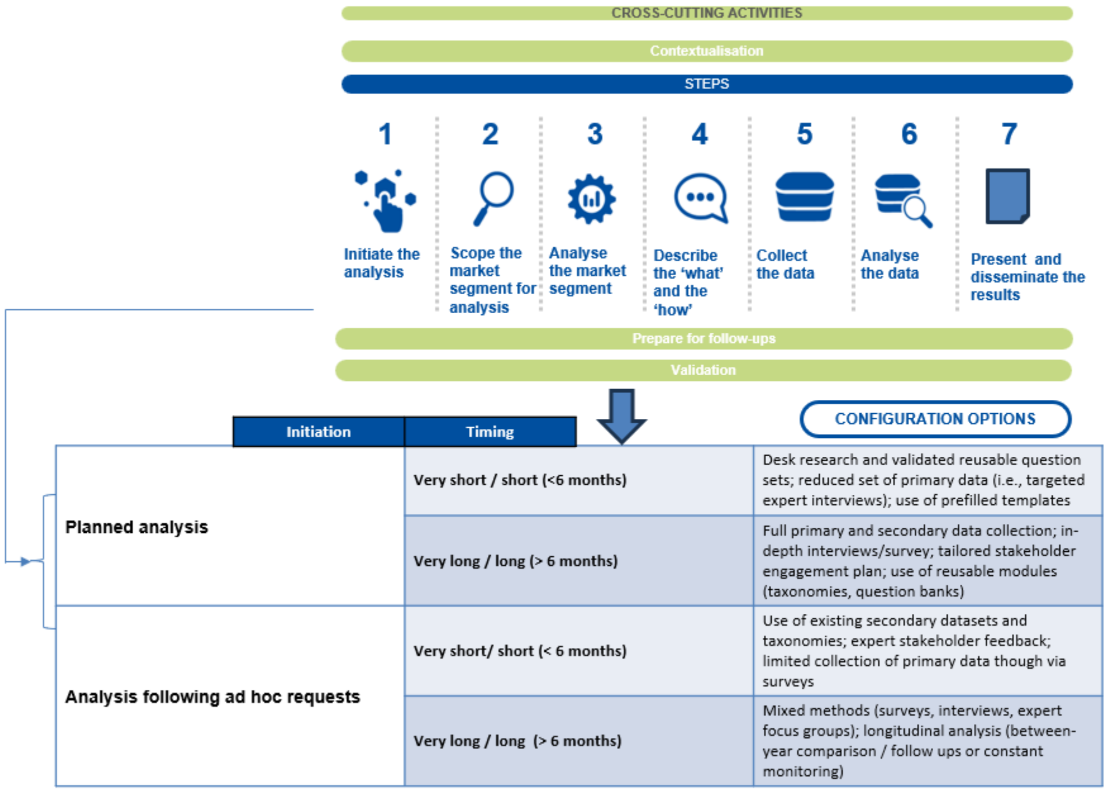
2. Overview of the Framework

The framework comprises the following seven steps:

- Step 1 – Initiate the analysis;
- Step 2 – Scope the market segment for analysis;
- Step 3 – Analyse the market segment;
- Step 4 – Describe the 'what' and the 'how';
- Step 5 – Collect the data;
- Step 6 – Analyse the data;
- Step 7 – Present and disseminate the results.

The ECSMAF steps are depicted in Figure 1. In the figure, the possible contexts of initiation and durations are shown, alongside some details of these options. A detailed description of the options for configuring the analysis by step are presented in the rest of this document, in particular in the chapters 'Planned Analyses (Short and Long Duration)' and 'Analyses Following Ad Hoc Requests (Short and Long Duration)'.

Figure 1: Overview of steps and configuration options for cybersecurity market analysis



Initiation	Timing	
Planned analysis	Very short / short (<6 months)	Desk research and validated reusable question sets; reduced set of primary data (i.e., targeted expert interviews); use of prefilled templates
	Very long / long (> 6 months)	Full primary and secondary data collection; in-depth interviews/survey; tailored stakeholder engagement plan; use of reusable modules (taxonomies, question banks)
Analysis following ad hoc requests	Very short/ short (< 6 months)	Use of existing secondary datasets and taxonomies; expert stakeholder feedback; limited collection of primary data though via surveys
	Very long / long (> 6 months)	Mixed methods (surveys, interviews, expert focus groups); longitudinal analysis (between-year comparison / follow ups or constant monitoring)

2.1 Workflow

As defined previously (see Figure 1), the application of the workflow in each of these steps depends on the configuration selected. It mainly depends on the initiation of the analysis and on the parametrisation of duration reflected in the given time constraints.

The differences in the pathway adopted are articulated throughout the seven-step workflow, and particularly in Step 1 (Initiate the analysis).

Step 1 (Initiate the analysis) differs substantially depending on whether the analysis is planned or conducted in response to an ad hoc request. In a planned analysis, initiation is anchored in ENISA's strategic programming and forward-looking priorities. The task of the analysis is to establish the analytical goal in line with the Agency's mandate, assess which segments or technologies are most relevant, define validation criteria and select the target segment by means of a documented rationale.

In contrast, the initiation of an ad hoc analysis begins with the request itself. The analyst's first responsibility is to capture and clarify the requestor's requirements, and then they must refine the scope to what is feasible with the available resources and time.

Step 1 (Initiate the analysis) and **Step 2** (Scope the market segment for analysis) set the parameters of the entire market analysis effort. These steps set the topic, breadth and depth of the analysis and determine the resources needed – that is, in terms of time, budget, human resources and tools.

Step 3 (Analyse the market segment) involves taking a closer look at the market segment and all its elements, including the infrastructure or architecture of supply chains, value stacks (i.e. services offered), assets, threats to those assets and security controls protecting the assets, and providing a snapshot of the major market stakeholders.

The combined outputs of the first three steps influence the structured formulation of questions in **Step 4** (Describe the 'what' and the 'how') by shaping the scope of the analysis, and by covering the elements of the market segment and the types of stakeholders who can provide support when addressing the research questions.

Step 5 (Collect the data) is the actual process of data collection, using the questions developed in **Step 4** (Describe the 'what' and the 'how)', but also other primary and secondary research (see Annex J 'Methodology').

Following data collection, **Step 6** (Analyse the data) comprises data analysis efforts, with a view to achieving the analysis target in accordance with the predetermined scope. This step includes the identification of interesting findings and the structuring of identified topics or outputs of the analysis.

Step 7 (Present and disseminate the results) involves careful consideration of how the outputs of the analysis are presented, including potential audiences, timelines and formats.

2.2 Actions

Each step of ECSMAF involves a set of actions. These actions are concrete tasks that guide the analysts' processes in a systematic and replicable manner. They ensure that each phase is actionable, clearly laid out and aligned with the methodological standards of the framework. Actions marked with 'where applicable' are optional – that is, they are not part of the standard workflow but may be incorporated when required by the analysis.

2.3 Cross-cutting Activities

While the ECSMAF process is articulated into a linear sequence of seven analytical steps (each of them operationalised through specific actions), each step is continuously supported by a set of cross-cutting activities that ensure methodological coherence, contextual sensitivity and practical relevance across the life cycle of the analysis. In particular, the following cross-cutting activities are envisaged.

- **Contextualisation** that ensures that each step of the analysis is grounded in an informed understanding of the broader landscape in which the market operates. This includes monitoring macroeconomic trends, regulatory developments, geopolitical shifts and the evolution of emerging technologies. It also entails evaluating the potential impact of disruption to the segment in question, recognising that a cyberattack on a critical infrastructure component differs significantly from one targeting a smaller, non-essential entity. When implementing ECSMAF, analysts are expected to embed the appropriate context (political, economic, social, technological, legal and environmental) into their scoping, prioritisation and interpretation choices (see Annex E 'Criteria for scoping the market analysis').
- **Validation** involves the systematic engagement of internal and external stakeholders to align assumptions, refine scoping parameters and verify outputs. From ensuring alignment with priorities (Step 1), to testing the relevance of scoping criteria (Step 2), validating infrastructure maps (Step 3), fine-tuning stakeholder questions (Step 4), cross-checking preliminary findings (Steps 5 and 6) and reviewing visualisations and results (Step 7), validation loops ensure that the analysis remains credible, consistent with its objectives and accountable to its beneficiaries. Validation is supported by quality assurance criteria, which ensure that the framework delivers outputs robust enough to support a reliable market analysis. Beyond stakeholder alignment and iterative review, minimum quality thresholds should be established, for example including the number of data collected, the variability of sources sufficient to enable pattern recognition and the consideration of data decay over time in relation to the analysis window.
- **Preparation for follow-ups** involves recognising that the value of market analyses often extends beyond immediate outputs. By documenting methods, generating lessons learned and structuring results in a way that can be reused or adapted for future studies, this activity embeds the analysis in a longer-term institutional learning cycle. It also ensures that appropriate formats, templates and walk-throughs are available for subsequent dissemination, knowledge transfer and refinement.

2.4 Timeline

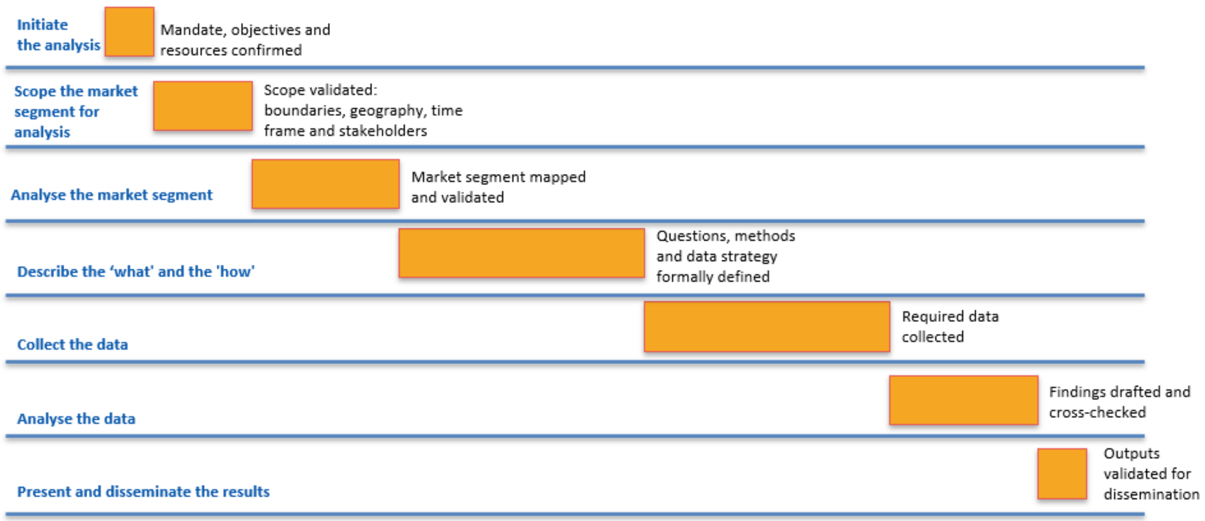
While the actual duration of each step may vary depending on the use case configuration, time constraints and data availability, a tentative timeline – based on previous experience of conducting market analyses – can be inferred by estimating the effort required for each step.

Broadly speaking, the most resource-intensive parts of the process are Step 4 (Describe the 'what' and the 'how') and Step 5 (Collect the data), which together may account for nearly half of the total time invested in each analysis.

These steps form the operational core of the market analysis, as they translate the defined scope into points of actions and generate the evidence base on which conclusions are built. Step 6 (Analyse the data) is also significant, though its duration typically correlates with the quality and structure of the data collected. Indicative step durations can be used as a high-level planning aid and adjusted based on the specific requirements and complexity of the market segment under investigation.

2.5 Indicative Time Allocation

Figure 2: Indicative duration of steps


Initiate the analysis
Mandate, objectives and resources confirmed
Scope the market segment for analysis
Scope validated: boundaries, geography, time frame and stakeholders
Analyse the market segment
Market segment mapped and validated
Describe the 'what' and the 'how'
Questions, methods and data strategy formally defined
Collect the data
Required data collected
Analyse the data
Findings drafted and cross-checked
Present and disseminate the results
Outputs validated for dissemination

The distribution of time slots for each step over the total time of an analysis (see Figure 2) is based on experience gained through a series of market analysis projects at ENISA and is merely indicative. For instance, the effort required for planned, long cybersecurity market analyses conducted by ENISA is around 15 person-months, over a period of around 10 months. The effort needed for the single ad hoc, short cybersecurity market analysis performed so far was around six person-months, conducted over a period of four months.

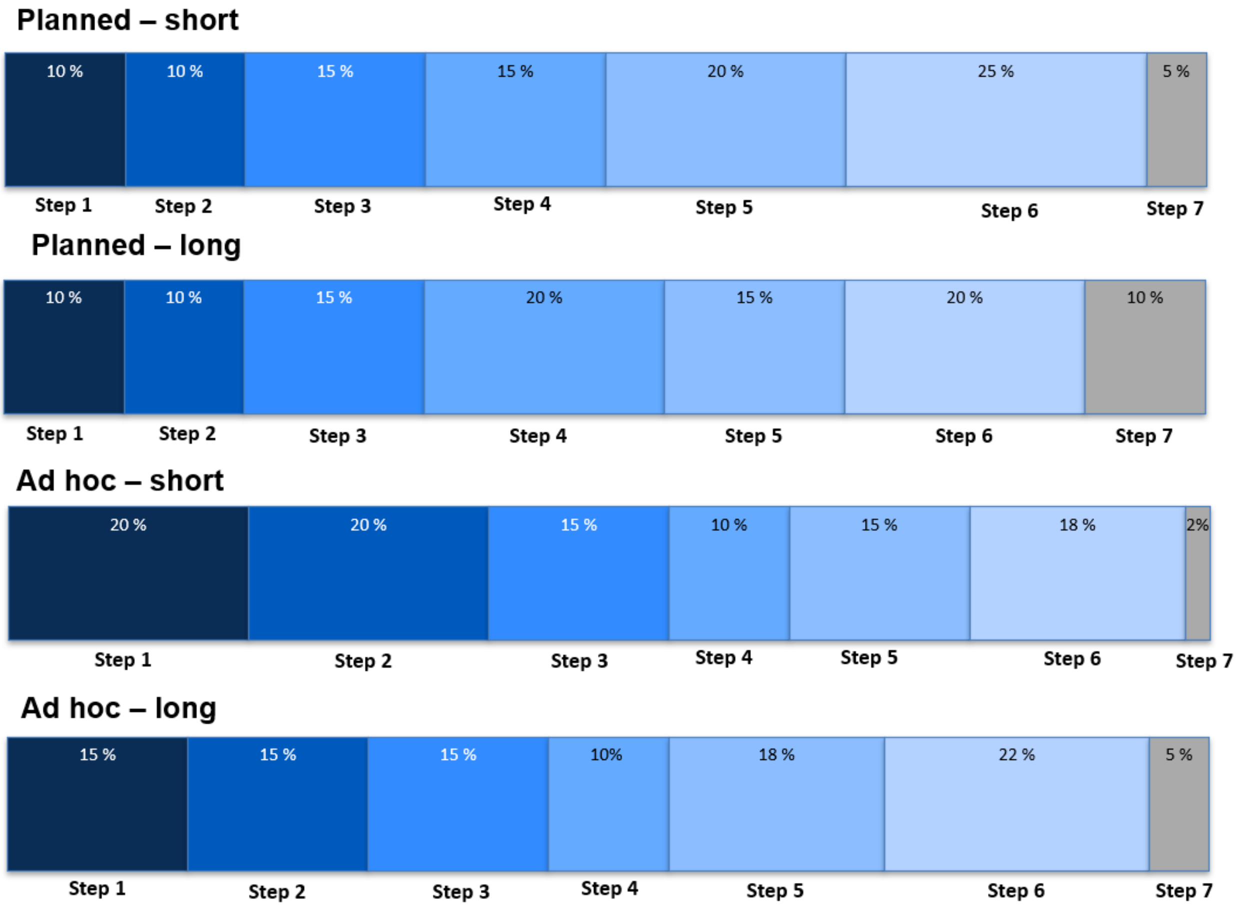
The duration of the analysis depends heavily on the resources allocated in terms of person-months, the data available, the procurement of services (e.g. support for data collection and analysis), the engagement of the requestor (in analyses following ad hoc requests), the support of an ad hoc working group, etc.

The actual duration of steps may also vary depending on the configuration and context of the analysis.

For instance, the initiation phase may require a significantly higher share of time if the exercise is conducted in response to an ad hoc request and if the initial request does not provide all the necessary information to scope the market segment effectively.

In addition to the allocation of time to the seven ECSMAF steps, the analyst(s) must consider the time required for cross-cutting activities (contextualisation, validation and preparation for follow-ups), based on the specific scope/needs of the market analysis.

Figure 3: Examples of allocation of time per configuration



As shown in Figure 3, the time allocated to an analysis varies depending on its configuration, reflecting whether it is ad hoc or planned, and whether it is short or long in scope.

- **Ad hoc analyses** are more front-loaded: initiation and scoping require a larger share of the effort, especially when initial requests require clarification. Dissemination, by contrast, is minimal, since outputs are tailored to the requestor, rather than shared with a broader stakeholder community.
- **Planned analyses** benefit from clearer mandates and predefined objectives, which reduce initiation time and allow for a more balanced distribution of time across the steps. In long configurations, more time is dedicated to dissemination and follow-up activities to maximise stakeholder engagement.
- **Short configurations** compress the data collection and analysis phases, while **long configurations** allow for deeper validation and reporting.

2.6 One-off and Recurrent Market Analysis and Continuous Market Monitoring

ECSMAF V3.0 supports one-off market analyses but also envisages the possibility of market analyses recurring over time, along with continuous market monitoring, enabling periodic updates and continuous observation of the same market segment as conditions evolve. This is further explained in a dedicated chapter later in this report (see the chapter ‘Towards Market Analysis Continuity: Recurrent Analyses and Continuous Market Monitoring’).

2.7 Tailoring of the Framework

ECSMAF has been developed with reference to ENISA's mandate and the needs of its stakeholders. However, the structure and logic of the framework are sufficiently generic to allow its application, with limited customisation, by organisations other than ENISA. National authorities, sectoral regulators, research institutes and private entities can all adapt the framework to guide their own cybersecurity market analyses.

Adhering to ECSMAF offers several advantages. It ensures a transparent and structured approach to market analysis; enhances the homogeneity of data across different studies and contexts, thus facilitating the comparability of conclusions; and facilitates the reusability of data and the transfer of knowledge between organisations. These benefits contribute to building a shared evidence base that can support decision-making at both the policy and the operational level.

However, some degree of tailoring may be required to reflect the specific needs, context or constraints of the organisation applying the framework. Adjustments may concern the scope of analysis, the depth of stakeholder engagement or the selection of data sources or methods. Such adaptations should remain consistent with the overall principles of ECSMAF, ensuring that the benefits of transparency, comparability and transferability are preserved.

Given the breadth of the EU's digital market and the need for scalable approaches, ECSMAF is also designed to be implemented at multiple levels. For example, ENISA could apply the framework to build capacities at the level of Member States, who in turn may conduct their own analyses locally. Synergistically, results can then be aggregated and compared across jurisdictions, thereby broadening participation, ensuring consistency and reinforcing the collective evidence base that underpins EU-level policy and strategy.

2.8 Annexes

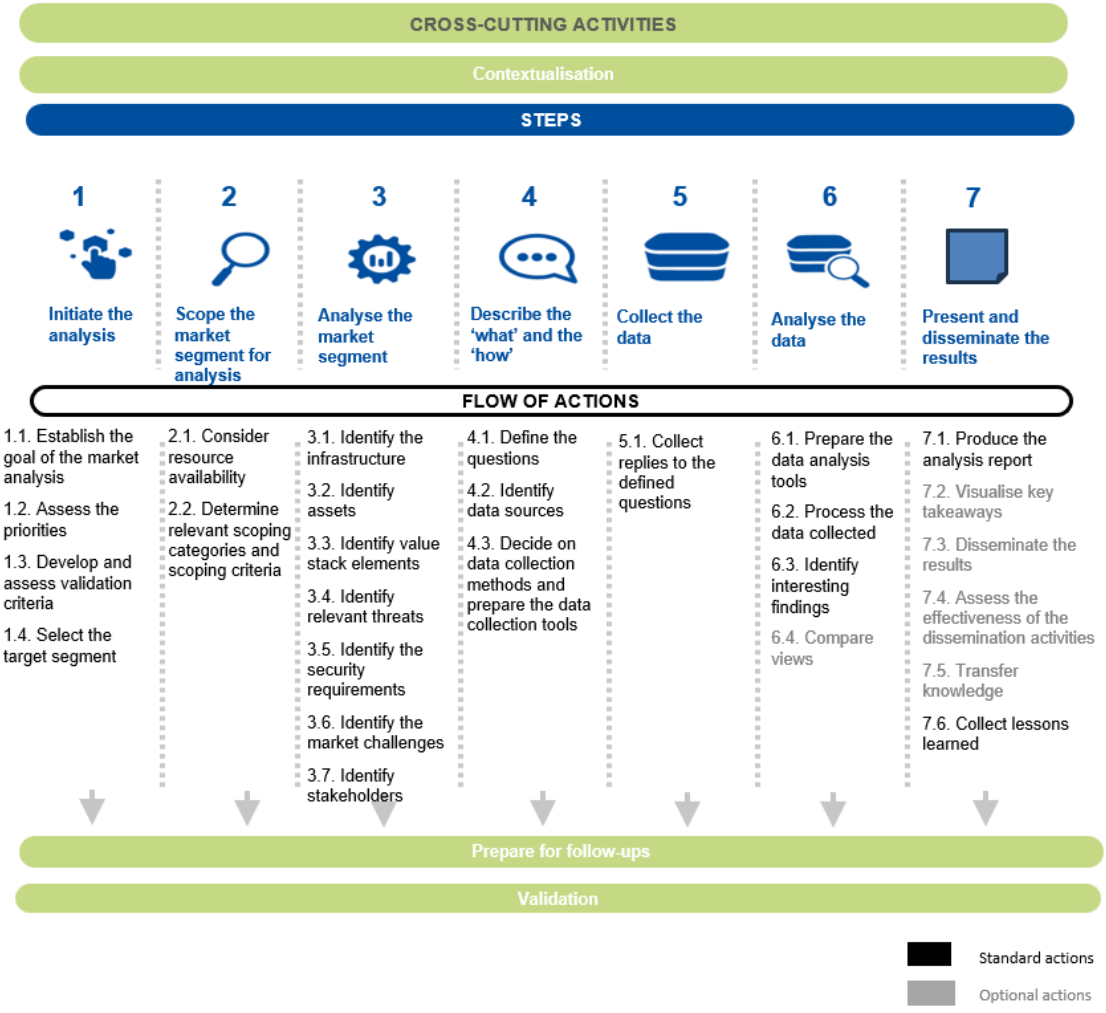
ECSMAF V3.0 contains some annexes that are drawn from the application of the previous versions of ECSMAF. The annexes support the application of ECSMAF. The number and content of the annexes is based on experience gained from previous market analyses. The annexes should be considered a developing part of this document, with some annexes and content to be added after further application of ECSMAF and based on the needs of analysts and stakeholders.

3. Planned Analyses (Short and Long Duration)

Planned analyses are market studies initiated by ENISA as part of its strategic planning to anticipate needs and support long-term monitoring. Analysts will find, in this section, descriptions of the specific actions each step entails; this section is followed by one detailing the actions to be taken in analyses following ad hoc requests, with a particular focus on the differences between configurations.

Descriptions of activities may include references to annexes that can be found at the end of the document. The annexes provide useful taxonomies or templates, where appropriate. An overview of the steps and actions to be taken during planned analyses is shown in Figure 4.

Figure 4: Overview of steps and actions involved in planned analyses


CROSS-CUTTING ACTIVITIES
Contextualisation
STEPS
1
Initiate the analysis
2
Scope the market segment for analysis
3
Analyse the market segment
4
Describe the 'what' and the 'how'
5
Collect the data
6
Analyse the data
7
Present and disseminate the results
FLOW OF ACTIONS
1.1. Establish the goal of the market analysis
1.2. Assess the priorities
1.3. Develop and assess validation criteria
1.4. Select the target segment
2.1. Consider resource availability
2.2. Determine relevant scoping categories and scoping criteria
3.1. Identify the infrastructure
3.2. Identify assets
3.3. Identify value stack elements
3.4. Identify relevant threats
3.5. Identify the security requirements
3.6. Identify the market challenges
3.7. Identify stakeholders
4.1. Define the questions
4.2. Identify data sources
4.3. Decide on data collection methods and prepare the data collection tools
5.1. Collect replies to the defined questions
6.1. Prepare the data analysis tools
6.2. Process the data collected
6.3. Identify interesting findings
6.4. Compare views
7.1. Produce the analysis report
7.2. Visualise key takeaways
7.3. Disseminate the results
7.4. Assess the effectiveness of the dissemination activities
7.5. Transfer knowledge
7.6. Collect lessons learned
Prepare for follow-ups
Validation
Standard actions
Optional actions

Planned analyses can be short or long in duration based on time constraints, depth of analysis, resource availability and intended audience. A short, planned analysis delivers focused insights within a limited time frame, while a long one provides a comprehensive, in-depth exploration of the selected market segment.

The planned analysis pathway supports the exploration of market segments as part of ENISA's activities. Planned analyses are designed to anticipate policy needs, support long-term monitoring and align with the agency's broader work programme.

3.1 Distinction between Short and Long Duration of Planned Analyses

In principle, short- and long-duration planned analyses share the same number of actions. The difference lies mainly in the effort invested in those activities.

A short (less than six months in duration) planned analysis is typically scoped to provide timely insights within an established strategic priority area. It applies existing methodologies and frameworks with limited customisation, focuses on essential stakeholder groups and delivers concise and focused outputs to inform specific policy discussions or internal needs.

A long (more than six months in duration) planned analysis, in contrast, is structured as a comprehensive exploration of the selected segment. It allows for deeper scope, expanded stakeholder consultation, multilayered validation and the integration of diverse data sources. The output is a detailed, methodologically robust deliverable designed to inform not only immediate policy needs but also medium- to long-term strategic reflections. The distinction between short and long formats lies in the breadth of stakeholder engagement, the degree of methodological adaptation, the volume of data collected and the level of granularity in the insights generated, rather than in the core analytical rigour.

Differences in the time allocated to steps in short- and long-duration analyses are shown in figures in the chapter 'Overview of the Framework': while **Figure 2** provides indicative durations for each step, **Figure 3** shows differences in the times allocated for short and long planned analyses.

3.2 Recurrent and Continuous Market Monitoring in Planned Analyses

A planned analysis may be a one-off or recurrent. In other words, it may be repeated over time. Recurrence and continuous monitoring are addressed in detail in the chapter 'Towards Market Analysis Continuity: Recurrent Analyses and Continuous Market Monitoring'.

3.3 Step 1: Initiate the Analysis (Planned)

The purpose of Step 1 of the planned analysis process is to define and structure the analytical direction of the market study. This phase ensures that the analysis is aligned with ENISA's mandate and strategic priorities and provides clear justification for the selection of the market segment (subset of the larger market that shares common needs and behaviours) to be examined. Each action progressively refines the focus, anchoring it to organisational priorities, validation requirements and a documented rationale for segment selection.

The actions involved in this step are listed below, with the following sections providing a detailed description:

- Action 1.1 – Establish the goal of the market analysis;
- Action 1.2 – Assess the priorities;
- Action 1.3 – Develop and assess validation criteria;
- Action 1.4 – Select the target segment.

3.3.1 Action 1.1: Establish the goal of the market analysis

The process begins by defining the overarching goal of the market analysis, specifying the desired outcomes and the expected contribution to ENISA's mission. The objective is to articulate a clear and strategically aligned goal that will guide the subsequent scoping and analytical efforts. A conditional check (to verify whether a certain condition is met) is performed to ensure that the goal of the analysis is clearly defined and aligned with ENISA's priorities. Only if the goal of the analysis is clearly defined and aligned with ENISA's priorities can we proceed to the next step. If the goal is too broad or vague, its scope should be narrowed down and made more specific. If there are multiple competing goals, they are prioritised based on ENISA's mandate and priorities. If overlaps with past studies are detected, the goal is reframed to highlight value added dimensions, such as updates or new analytical angles.

In the short configuration, this refinement process is tightly managed within predefined boundaries, relying on internal existing documentation and recent strategic outputs (e.g. ENISA's Single Programming Document[9], ENISA Strategy[10], etc) to accelerate decision-making.

In the long configuration, the process accommodates exploratory considerations, including horizon scanning through external resources (e.g. grey literature, radars, white papers) and internal research (e.g. ENISA's threat landscape report ([11]), the report *ENISA Foresight Cybersecurity Threats for 2030 – Update* ([12])), to iteratively refine the goal and ensure coherency with strategic foresight.

3.3.2 Action 1.2: Assess the priorities

Once the goal is consolidated, the next step is to assess which market segments or technologies, products, services and processes are most strategically important to analyse. This evaluation is conducted based on ENISA's current strategic priorities, which may deviate from the goals of the specific analysis. A conditional check here can ensure that there is a clear and uncontested priority for analysis. If conflict arises over priorities, the matter is escalated for internal review at the management level.

In the short configuration, the assessment is guided by pre-established strategic areas. Alignment is sought with the CSA and ENISA's strategic documents, for example the ENISA Strategy ([13]), ENISA's International Strategy ([14]) and ENISA's Stakeholders' Strategy ([15]); ENISA Single Programming Document ([16]); and ENISA's technology and innovation radar work ([17]) and work on foresight ([18]).

[9] ENISA, *ENISA Single Programming Document 2026 - 2028*, Publications Office of the European Union, Luxembourg, 2025, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA_Single%20Programming_Document_2026.pdf (accessed 11/03/2026).

[10] ENISA Strategy 'A Trusted and Cyber Secure Europe - ENISA Strategy', https://www.enisa.europa.eu/publications/a-trusted-and-cyber-secure-europe-enisa-strategy, accessed 11/03/2026.

[11] For more information on ENISA's threat landscape work, see ENISA, 'Threat landscape', ENISA website, https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape (accessed 25/09/2025).

[12] ENISA, *Foresight Cybersecurity Threats for 2030 – Update*, 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary (accessed on 21/10/2025).

[13] ENISA, *A Trusted and Cyber Secure Europe – ENISA strategy*, Publications Office of the European Union, Luxembourg, 2025, https://www.enisa.europa.eu/publications/a-trusted-and-cyber-secure-europe-enisa-strategy (accessed 22/07/2025).

[14] See *ENISA International Strategy 2026,* https://www.enisa.europa.eu/publications/enisa-international-strategy-2026 (accessed 11/03/2026).

[15] *ENISA Stakeholder Strategy 2026-2028*, https://www.enisa.europa.eu/publications/enisa-stakeholder-strategy-2026-2028 (accessed 11/03/2026).

[16] See ENISA, *ENISA Single Programming Document 2026 - 2028*, Publications Office of the European Union, Luxembourg, 2025, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA_Single%20Programming_Document_2026.pdf.

[17] See, for instance, ENISA's technology and innovation radar methodology (to be published).

[18] See, for instance, ENISA, *Foresight Cybersecurity Threats for 2030 – Update*, 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary (accessed on 21/10/2025).

In the long configuration, a more participatory approach is adopted, potentially involving, in addition to alignment with strategic documents, structured consultation across ENISA activities. The aim is to navigate competing priorities and ensure a balanced selection reflective of the wider field of cybersecurity.

3.3.3 Action 1.3: Develop and assess validation criteria

Following priority setting, validation criteria are defined to ensure that the planned analysis maintains its quality throughout execution. These criteria establish the standards by which the scope, methods and outputs will be assessed at key checkpoints. At this point, the analyst checks whether clear, context-appropriate validation criteria are already defined. If such criteria do not exist, they are built based on experience from previous cycles. If there is found to be too many criteria, which may dilute the focus of the analysis, the most important are prioritised. If criteria rely on unavailable information, proxy indicators should be used to ensure the validity of assumptions.

In the short configuration, criteria are typically adapted from existing analyses, ensuring consistency and expediting their definition and volume.

The long configuration supports a more tailored approach, introducing bespoke criteria (e.g. a minimum number of specific stakeholders required to validate the data collected or the findings). These criteria are determined by the specific characteristics of the segment targeted, policy relevance and anticipated analytical depth.

3.3.4 Action 1.4: Select the target segment

With the goal, priorities and validation criteria established, the target market segment is selected. The selection is justified through a documented rationale linking to the strategic priorities and validated criteria. A conditional check is conducted to assess whether a clear segment has been chosen without overlaps or structural concerns. If multiple segments remain under consideration, internal scoring is conducted to prioritise them (see Annex D ‘Template for Assessing the Priority of Market Segments’).

Should structural issues be identified, for example feasibility risks or lack of data, the selection is tested against exposure trends ([19]), technological maturity ([20]) or early warnings ([21]).

Where overlaps with other EU initiatives are present, coordination with relevant internal and external actors is initiated to define synergies or delineate boundaries.

In the short configuration, segment selection is formalised through expedited scoring and risk screening, ensuring the process concludes within a defined timeline.

In the long configuration, the evaluation is deeper and may involve iterative expert reviews and scenario analysis to confirm the robustness of the chosen segment and its alignment with strategic trends at the EU level.

[19] To test the selection of the segment for issues such as feasibility risks or lack of data, analysts can use the biennial technical report on emerging cybersecurity risks, which ENISA is tasked with preparing under the CRA (see Art. A17, para. 3, and Recital 69), along with ENISA’s work on situational awareness (ENISA, ‘Situational awareness’, ENISA website, https://www.enisa.europa.eu//topics/cyber-threats/situational-awareness, accessed 11/03/2026).

[20] See ENISA’s technology and innovation radar methodology (to be published).

[21] To test the selection of the segment for issues such as feasibility risks or lack of data, analysts can use data from the European Union Vulnerability Database (https://euvd.enisa.europa.eu) and ENISA’s situational awareness work (ENISA, ‘Situational awareness’, ENISA website, https://www.enisa.europa.eu//topics/cyber-threats/situational-awareness) can be used (accessed 11/03/2026).

3.3.5 Validation

To conclude Step 1, a check is conducted to ensure that the goal, priorities, validation criteria and segment selection are coherent and aligned with ENISA's broader strategic orientation.

In the short configuration, validation is internal and relies on the analysis team's assessment against pre-agreed strategic markers.

The long configuration extends this validation to include strategic advisory inputs (e.g. from ENISA's Advisory Group ([22]), ENISA's National Liaison Officers Network ([23]) or ad hoc thematic working groups), cross-unit feedback within ENISA, and, where relevant, consultation with external policy or industry experts.

3.3.6 Prepare for follow-ups

This step proposes potential follow-up measures that may be necessary due to evolving priorities, policy changes or the encountering of unforeseen challenges.

In the short configuration, follow-ups are typically captured in internal records, with clear notes on decision points and potential contingencies.

In the long configuration, a structured follow-up mechanism is instituted, potentially including scheduled review milestones, stakeholder re-engagement strategies and the formal tracking of alternative segments or emerging issues for future analytical cycles.

3.3.7 Annexes relevant to Step 1

- Annex D – Template for Assessing the Priority of Market Segments
- Annex P – Practical Checklists for Analysts

3.4 Step 2: Scope the Market Segment for Analysis (Planned)

Once the choice of market segment has been validated and aligned with ENISA's strategic priorities (see Step 1), the selected market segment is scoped. This step ensures that the focus of the analysis is both feasible and analytically robust, given available resources and stakeholder expectations.

The actions involved in this step are listed below and described in the sections that follow:

- Action 2.1 – Consider resource availability;
- Action 2.2 – Determine relevant scoping categories and scoping criteria.

3.4.1 Action 2.1: Consider resource availability

The analyst begins by assessing the practical constraints of the analysis, including available time, internal expertise, and the ability to engage relevant stakeholders. These factors are used to calibrate the expected depth and breadth of the study, ensuring that the scope is realistic given operational capacities and ENISA's priorities. A conditional check is performed to determine whether the proposed analysis is comparable to any previous internal study. If the scope and analytical context align with past efforts, underlying assumptions regarding resource needs can be reused with minimal adjustment. In such cases, the process continues directly to defining the scope. However, if the

[22] For more information on ENISA's Advisory Group, see ENISA, 'Advisory group (AG)', ENISA website, https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag (accessed 25/07/2025).

[23] For more information on the National Liaison Officers Network, see ENISA, 'National Liaison Officers Network (NLOs)', ENISA website, https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/nlo-network (accessed 25/07/2025).

analysis is framed around a familiar topic but stakeholder expectations have shifted, these new priorities must be clarified and resource planning adapted accordingly. In situations where the scope introduces a novel domain or analytical challenge, the analyst should document the nature of the change or barrier and prepare a revised resource plan that reflects the emerging needs, including efforts to generate related material to cover the scope.

Once appropriately calibrated, the process advances to defining the scoping categories. The handling of resource availability differs between the short and the long configurations.

In the short configuration, the assessment of resources is deliberately streamlined, typically leveraging prior analyses or default assumptions to expedite scoping decisions. It may involve using secondary data (see Annex J 'Methodology') or rely on easily accessible internal expertise.

In contrast, **the long configuration** allows a more comprehensive assessment of resources, including the mapping of available external expertise, the identification of potential data gaps and formal consultation with relevant ENISA units or partners to secure specialised input.

3.4.2 Action 2.2: Determine relevant scoping categories and scoping criteria

With resource considerations in place, the next task is to define the analytical framing of the market analysis. This involves selecting the appropriate scoping categories (see Annex E 'Criteria for Scoping the Market Analysis') and criteria that will structure the forthcoming analysis. Categories typically define the boundaries and extent of the area of focus of the analysis. A conditional check is then used to verify whether the existing ECSMAF scoping categories are sufficient to accommodate the goal of the analysis. If they are, the existing framework is applied directly and the process continues to market segment analysis (Step 3 Analyse the market segment). If the market segment necessitates minor adaptations to the framing of the analysis – for instance, the reordering of criteria or the introduction of a new thematic emphasis – these changes are made while clearly documenting the deviation from the standard configuration. Once the revised categories are defined, the analyst proceeds to the next phase.

In the short configuration, the selection of scoping categories is typically constrained to predefined templates (see Annex E 'Criteria for Scoping the Market Analysis'), with minimal customisation to maintain pace. The analyst relies on knowledge available from previous applications of ECSMAF and avoids introducing new categories unless strictly necessary.

Conversely, **the long configuration** permits a more flexible and iterative approach, enabling the analyst to explore hybrid scoping models, integrate emerging thematic areas and engage stakeholders or domain experts in validating the chosen categories.

3.4.3 Validation

At the conclusion of Step 2, a check is conducted to confirm that the resource plan and the selected scoping categories are coherent, sufficient and aligned with the goal of the analysis and ENISA's strategic orientation.

In the short configuration, this validation is internal and expedited, generally involving the core analysis team conducting a final plausibility check. If the existing scoping criteria do not cover the desired focus, the analysis must loop back to Action 2.1 (Consider resource availability), as also mentioned in the cross-cutting activity 'Prepare for follow-ups'.

In the long configuration, the validation process may include a structured peer review or a formal check by relevant ENISA units, ensuring that both resource allocation and analytical framing are fit for purpose before the analysis phase begins.

3.4.4 Prepare for follow-ups

This step establishes the basis for any follow-ups related to resource constraints or scoping decisions.

In the short configuration, this may simply involve the noting of any compromises made or limitations accepted during the scoping process.

In the long configuration, more formal documentation is maintained, including an explicit record of resource dependencies, outstanding data needs or optional scoping areas that could be explored in subsequent cycles. This ensures that any deferred elements or residual uncertainties are flagged for potential revisit, either within the current cycle or in future iterations of the process.

3.4.5 Annexes relevant to Step 2

- Annex E – Criteria for Scoping the Market Analysis
- Annex P – Practical Checklists for Analysts

3.5 Step 3: Analyse the Market Segment (Planned)

With the scope defined and validated, the analysis moves on to characterising the selected market segment. In this step, the aim is to develop a grounded and structured understanding of the segment. The process follows a logical sequence of investigative actions, each designed to feed into a coherent market profile. The market segment is analysed based on the data already available. It can then be refined, as appropriate, based on additional data that will be collected under Step 5.

The actions involved in this step are listed below and described in the sections that follow:

- Action 3.1 – Identify the infrastructure;
- Action 3.2 – Identify assets;
- Action 3.3 – Identify value stack elements;
- Action 3.4 – Identify relevant threats;
- Action 3.5 – Identify the security requirements;
- Action 3.6 – Identify the market challenges;
- Action 3.7 – Identify stakeholders.

3.5.1 Action 3.1: Identify the infrastructure

The first analytical task is to map the infrastructure (see Annex F 'Infrastructure mapping') underpinning the selected market segment. This includes the technical components, systems, platforms and operational environments that define the segment's architecture. If the required information is readily available (either through existing studies, stakeholder inputs or documentation), the infrastructure is directly mapped. In the absence of reliable data, a new infrastructure map is developed based on the defined scope. This map serves as the backbone for subsequent asset identification. Given the cybersecurity focus of the analysis, this action aims to identify important (i.e. valuable) components of infrastructure that are exposed and require protection, in preparation for Action 3.2 (Identify assets) below.

In the short configuration, the mapping relies primarily on available data sources and previously validated studies, with limited effort devoted to constructing new maps unless critical gaps are identified.

The long configuration, in contrast, allows for the development of detailed infrastructure maps, the identification of cybersecurity requirements to be incorporated in the collection of primary data, expert interviews and the examination of indirect indicators, such as procurement data or patent analysis, to address potential protection limitations.

3.5.2 Action 3.2: Identify assets

Following infrastructure mapping, the analysis identifies key assets that enable or support the functioning of the segment and value creation within it. These may include products with digital elements, digital services, or human capital. The assets identified can be cross-validated by the appropriate stakeholders, depending on the timeline of the analysis. If agreement is not reached, expert triangulation is used to refine the asset list before proceeding.

When addressing the infrastructure of products with digital elements (categorised as important or critical products in accordance with Annex III (Important products with digital elements) and Annex IV (Critical products with digital elements) of the CRA ([24])), parts that could be considered assets have to be identified.

In the short configuration, assets are typically identified through desk research and internal validation, with the list kept concise and focused on the most critical assets.

In the long configuration, this step is expanded to include the application of structured methods for asset classification, for example more comprehensive desk research and the consultation of relevant experts and stakeholders.

3.5.3 Action 3.3: Identify value stack elements

The value stack analysis outlines the layered structure of the collection of services contributing to the value proposition of an organisation. The value stack bundles together products, services, processes or value streams (see Annex B ‘Glossary’) to increase the overall perceived value for a customer or user. This structured breakdown helps highlight interdependencies and areas of added value. When the structure of the value chain is already defined or recognised, it is documented directly. If the structure is ambiguous or fragmented, expert input or proxy indicators are used to reconstruct it.

In the short configuration, the value stack is documented using existing models or frameworks (see Annex G ‘Examples of Cybersecurity Value Stack) with minimal revision, ensuring rapid progression to subsequent actions.

The long configuration enables a deeper examination of the value stack, including the validation of layers and the integration of non-cyber value elements that may influence the market segment’s dynamics.

3.5.4 Action 3.4: Identify relevant threats

The threat landscape pertinent to the infrastructure being analysed is then assessed. Where the segment is linked to critical sectors or regulatory designations (e.g. critical infrastructure under the NIS 2 Directive ([25]), products considered critical under the CRA ([26])), the threat list is expanded to

[24] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj) (accessed 22/07/2025).

[25] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27) (accessed 22/05/2025).

[26] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj) (accessed 22/05/2025).

include both high-impact and low-probability scenarios. If no specific scoping conditions apply, threats are mapped to include cyber and non-cyber threats in the structure of the assessment.

In the short configuration, the threat assessment is conducted through existing taxonomies and scenario models, focusing on known and immediate risks.

In the long configuration, a more granular threat modelling exercise can be performed, which may include scenario-based analyses, workshops and the consideration of hybrid threats combining technical and other (e.g. societal) dimensions.

3.5.5 Action 3.5. Identify the security requirements

This action focuses on identifying cybersecurity requirements imposed by the kind of product or service, by the infrastructure and by the specific sector, as applicable. If stakeholders have already adopted a recognised baseline fulfilling these requirements, it is documented and incorporated in the analysis. Where comparable past analyses exist, requirements and controls from analogous segments may be reused. In novel cases, secondary data are used to derive a provisional list of security requirements, which is then validated through expert engagement or stakeholder consultation. Moreover, depending on the scope of the analysis, it should consider requirements addressed in emerging, community-driven standards and compliance toolkits developed by standardisation bodies (e.g. open-source stewardship bodies) ([27]).

In the short configuration, the security requirements are derived primarily from legislation (the NIS 2 Directive ([28]) and the CRA ([29])), existing certification schemes, existing relevant standards, baseline protection measures and technical specifications, or previous ENISA studies.

The long configuration supports a more bespoke approach, expecting the analyst to propose tailored security requirements to ensure relevance and completeness.

3.5.6 Action 3.6: Identify the market challenges

Market challenges are then assessed to identify systemic or operational barriers affecting the segment. These may relate to fragmentation, lack of incentives, barriers to market entry, skills shortages, regulatory gaps, sectoral maturity (if applicable), technological immaturity (as established by the technology and innovation radar ([30])), cybersecurity risks (indicated, for example, by market trends or consumer complaints) ([31]), innovation gaps, etc. Where known challenges exist, they are clustered by type and impact. If no challenges are evident or the information is unavailable, the analysis proceeds directly to stakeholder mapping.

In the short configuration, challenges are identified based on secondary sources, focusing on the most frequently cited barriers (see Annex I ‘Barriers and challenges’)

([27]) For example, the EU-funded Eclipse Foundation open source compliance comprehensive tools and resources (OCCTET) project, the Open Source Security Foundation’s Linux Foundation Express Learning 1001 course and specifications from the Eclipse Open Regulatory Compliance Working Group.

([28]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27) (accessed 22/07/2025).

([29]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj), (accessed 22/05/2025).

([30]) See ENISA’s technology and innovation radar methodology (to be published).

([31]) The biennial technical report on emerging cybersecurity risks, which ENISA is tasked with preparing under the CRA (see Art. A17, para. 3, and Recital 69) is an important document to consider when addressing the cybersecurity risks.

In the long configuration, the assessment is enriched with direct expert feedback and through the application of analytical tools, to classify and prioritise challenges based on their impact and tractability.

3.5.7 Action 3.7: Identify stakeholders

The final action of Step 3 maps the those involved in or affected by the market segment. This typically includes supply-side and demand-side stakeholders, regulatory bodies, and research and development institutions. If stakeholders' roles and relationships are already clear, they are mapped directly. If they are not, stakeholder groups are categorised using structured tools such as power–interest matrices, ensuring that their roles are adequately captured to facilitate subsequent engagement.

When identifying stakeholders, special attention should be given to start-ups and scale-ups, since they play an important role in innovation.

In the short configuration, stakeholder mapping ([32]) is concise, focusing on key institutional actors and primary market participants.

The long configuration allows for more extensive mapping, capturing a broader array of stakeholders, including emerging actors and non-traditional participants. Their categorisation is supported by additional network analyses (see Annex J 'Methodology'), where necessary.

3.5.8 Validation

At the conclusion of Step 3, a check is conducted to ensure the completeness and accuracy of market segment characterisation.

In the short configuration, validation is performed internally by the analysis team, possibly supplemented by a brief consultation with a few subject matter experts, and/or feedback from a relevant ad hoc group (e.g. ENISA's Ad Hoc Working Group on the EU Cybersecurity Market).

The long configuration employs a more formal validation process, including structured feedback sessions with relevant experts and cross-validation against external data sources.

3.5.9 Prepare for follow-ups

This step concludes with the preparation for follow-up measures, particularly regarding any data gaps identified, contested findings, areas requiring further investigation, and continuing the analysis, where appropriate, jointly with other stakeholders or by other stakeholders.

In the short configuration, follow-up measures are typically documented as suggestions for future analysis cycles.

In the long configuration, a more detailed follow-up plan is drafted, which may include targeted data collection exercises, the establishment of ongoing stakeholder dialogues, or the scheduling of update cycles to capture the change in the segment over time.

3.5.10 Annexes relevant to Step 3

- Annex B – Glossary
- Annex F – Infrastructure Mapping
- Annex G – Examples of Cybersecurity Value Stacks

[32] ENISA Stakeholder Strategy 2026-2028 (https://www.enisa.europa.eu/publications/enisa-stakeholder-strategy-2026-2028, accessed 11/03/2026) is an important document to consider when mapping stakeholders.

- Annex H – Stakeholders
- Annex I – Barriers and Challenges
- Annex J – Methodology
- Annex P – Practical Checklists for Analysts

3.6 Step 4: Describe the 'What' and the 'How' (Planned)

With the analytical scope in place, Step 4 involves defining the guiding questions, identifying relevant data sources and selecting appropriate data collection methods. The goal of this step is to ensure that the forthcoming data collection and related stakeholder engagement are targeted, relevant and adapted to the analysis context.

The actions involved in this step are listed below and described in the sections that follow:

- Action 4.1 – Define the questions;
- Action 4.2 – Identify data sources;
- Action 4.3 – Decide on data collection methods and prepare the data collection tools.

3.6.1 Action 4.1: Define the questions

The analyst begins by formulating a set of questions. These questions should reflect the specific scoping elements of the analysis and be calibrated to the types of stakeholders involved. If both scope and stakeholders are comparable to a previous ENISA market analysis, the same questions can be used. If the scope is different, the existing questions should be reprioritised and adjusted. If new stakeholders are involved, additional targeted questions are incorporated. Where both the scope and the stakeholder landscape differ significantly, a full overhaul of the question set is required.

In the short configuration, the question set (see Annex L 'Examples of Survey Questions for Each Stakeholder Type') is kept streamlined, typically limited to a core selection of predefined or previously validated questions to ensure rapid progression to the next stage of the analysis. Questions are adapted only when critical to address variations in scope.

The long configuration enables a more expansive and tailored approach, including the development of exploratory prompts (see Annex B 'Glossary') to capture emerging issues or underexplored dimensions.

3.6.2 Action 4.2: Identify data sources

Once the questions are decided, the analyst identifies where the data required to answer them can be found, and compiles a list of data sources (see Annex J 'Methodology') to support the analysis. The sources may include previous ENISA studies, academic literature, official statistical repositories, regulatory documents, proprietary datasets, expert contacts and sector-specific insights. Mapping data sources at this stage helps structure stakeholder engagement and ensures that stakeholders' inputs complement rather than duplicate existing evidence.

When mapping the data sources, analysts should consider whether the data are provided on a voluntary basis or as part of a structured mandatory reporting mechanism, and whether they are provided on an ad hoc basis or on a regular basis.

In the short configuration, the mapping of data sources focuses on immediately available and predefined materials.

The long configuration allows for the broader and more systematic identification of data sources, including the exploration of grey literature (see Annex B 'Glossary'), and the establishment of new data partnerships (e.g. agreements with database providers) if required.

3.6.3 Action 4.3: Decide on data collection methods and prepare the data collection tools

The final preparatory action involves selecting data collection methods and designing the appropriate tools for collecting the data from the sources identified in Action 4.2 (Identify data sources) and based on the questions formulated in Action 4.1 (define the questions).

The choice of method (see Annex J 'Methodology') depends on the timeline and goals of the analysis and expected stakeholder availability. Where extensive engagement is feasible, a detailed survey is deployed. If time is more constrained, focused interviews or moderated workshops are organised. Where limited engagement is anticipated, leaner approaches using publicly available data or data already available from other sources (including data collected by ENISA or available from other external sources), brief surveys and expert validation rounds are to be adopted. The methods selected are then operationalised through well-designed instruments aligned with the scope and questions defined earlier.

In the short configuration, the data collection method is chosen for its speed and minimal burden on stakeholders, often relying on publicly available data, short-form surveys or a limited number of interviews. Tools are typically chosen from existing templates (see Annex K 'Data Collection') to avoid delays.

In the long configuration, method selection is more flexible and may involve mixed methods approaches, combining surveys, interviews and focus groups. The tools are also more extensively customised, with the possibility of conducting pilot testing to ensure the clarity and relevance of methods and their alignment with the diverse stakeholder profiles involved.

3.6.4 Validation

Step 4 concludes with a check aimed at ensuring the consistency and quality of the data, but also adequate representation of sources, and that methods for engaging with sources are robust and aligned with both the scope of the analysis and the analytical objectives set.

In the short configuration, this validation is carried out internally by the analysis team, focusing on consistency and feasibility.

The long configuration includes an additional layer of validation, such as seeking feedback from selected stakeholders or internal reviewers to confirm the appropriateness of the engagement strategy before deployment.

3.6.5 Prepare for follow-ups

This step also includes preparatory actions for potential follow-ups.

In the short configuration, preparation for follow-ups is limited to noting any anticipated gaps in or challenges to stakeholder participation and having contingencies in place, such as alternative data sources or simplified collection instruments (e.g. open-source data).

In the long configuration, a more comprehensive follow-up plan is developed, including strategies for re-engagement, iterative data collection rounds and mechanisms for adapting tools and methods based on initial stakeholder feedback or response rates.

3.6.6 Annexes relevant to Step 4

- Annex B – Glossary
- Annex J – Methodology

- Annex K – Data Collection
- Annex L – Examples of Survey Questions for Each Stakeholder Type
- Annex P – Practical Checklists for Analysts

3.7 Step 5: Collect the Data (Planned)

With the data sources and data collection methods identified and the relevant tools prepared (e.g. the EUSurvey tool), the analysis proceeds to data collection. This phase may involve engaging stakeholders directly to capture input on the questions defined during the preparatory stage. The objective is to gather reliable, accurate and targeted information that will enrich the desk research and support the development of a robust market analysis.

Market analysts can gather the data they need for their analyses by a variety of means and from a variety of sources. They can conduct either primary or secondary research.

- **Primary research** is conducted through surveys, interviews, focus groups and observation. These activities are performed directly by the owner of the market analysis, who is also the data owner. Surveys, interviews and focus groups are examples of primary (or empirical) research.
- **Secondary research** is conducted by collecting data from already available sources, such as online communities, contractors and automated/manual open-source searches. The owner of the market analysis does not own the material collected from secondary research. A literature review is an example of secondary research.

The action involved in this step is Action 5.1 (Collect replies to the defined questions).

3.7.1 Action 5.1: Collect replies to the defined questions

Stakeholder engagement is carried out using the selected methods. Regardless of the method, the input collected is documented systematically and checked for consistency.

Throughout this phase, it is essential to keep track of the data collection methodology (see Annex K ‘Data Collection’) through appropriate documentation. This includes keeping records of the tools used, the criteria for selecting stakeholders, formats for stakeholder engagement and any deviations from the planned process.

In parallel, all data collection activities (in both the short and the long configuration) must be conducted in line with appropriate regulations, for example concerning stakeholder engagement, data privacy and intellectual property rights. This entails securing informed consent, ensuring confidentiality where applicable and aligning the engagement approach with ENISA’s ethical standards and regulatory obligations.

In the short configuration, data collection is typically limited in duration and scope, focusing on a restricted set of stakeholders identified as critical to the market segment. Existing data (e.g. publicly available or available within ENISA, provided that they can be reused for the purpose of the analysis) should be used. The engagement of stakeholders can be also considered, and can be conducted through streamlined formats such as brief surveys or short interviews, prioritising speed and responsiveness over depth of responses.

In the long configuration, the process allows for broader and more diverse stakeholder participation, employing multiple engagement formats, such as interviews and focus groups, where needed.

3.7.2 Validation

At the conclusion of the data collection process, a check is conducted to verify the completeness and integrity of the data gathered.

In the short configuration, this validation consists of an internal review by the analysis team to confirm that the data sufficiently cover the key questions and stakeholder perspectives.

In the long configuration, validation may also involve a preliminary synthesis of responses shared with selected internal stakeholders, and external experts if needed.

3.7.3 Prepare for follow-ups

Data collection concludes with the preparation for potential follow-up measures.

In the short configuration, this may involve simply identifying any areas where stakeholder responses were incomplete or unclear, with ad hoc clarification sought if time allows. Should the validation of the data collection process (see the section on this cross-cutting activity above) indicate shortcomings in data quality or stakeholder participation, steps need to be taken to mitigate their impact.

In the long configuration, a structured follow-up plan is developed, potentially including the scheduling of additional rounds of engagement, the submission of supplementary data requests or the design of targeted consultations to address residual data gaps identified during the initial data collection phase.

3.7.4 Annexes relevant to Step 5

- Annex K – Data Collection
- Annex P – Practical Checklists for Analysts

3.8 Step 6: Analyse the Data (Planned)

Once data collection is complete, the analysis progresses to processing and interpreting the information gathered. This step ensures that the data are made usable, cross-validated across sources and transformed into meaningful insights.

The actions involved in this step are listed below and described in the sections that follow:

- Action 6.1 – Prepare the data analysis tools;
- Action 6.2 – Process the data collected;
- Action 6.3 – Identify interesting findings;
- Action 6.4 – Compare views (where applicable).

3.8.1 Action 6.1: Prepare the data analysis tools

Before the analysis begins, appropriate tools must be selected and prepared based on the type of data collected, the time available, the desired depth of insight and the structure of the analysis. These tools may include structured templates (see Annex K ‘Data Collection’), qualitative coding schemes (systems for categorising and labelling textual or interview data) (see Annex M ‘Coding Schemas’) or quantitative processing utilities (tools for handling numerical data and performing statistical analysis). Once the tools are ready, the analysis can proceed.

In the short configuration, data analysis tools are selected based on efficiency, often including predefined templates and rapid coding mechanisms that accommodate both qualitative and quantitative data without extensive customisation.

In the long configuration, the selection is tailored to support the integration of diverse data types and the exploration of complex interdependencies within the dataset.

3.8.2 Action 6.2. Process the data collected

The raw data are then organised, cleaned and structured to facilitate interpretation. This includes removing redundancies, harmonising formats and clustering the information in a way that enables meaningful comparison across sources (see Annex K 'Data Collection').

In the short configuration, standardisation and quick formatting are prioritised in data processing to enable immediate interpretation. Processing steps are focused on ensuring the completeness and consistency of data, and do not involve extensive reclassification or reformatting.

In the long configuration, more comprehensive data cleaning and structuring efforts are conducted, including the application of coding schemes for qualitative data, statistical normalisation for quantitative inputs and the creation of comparative datasets to support multidimensional analysis.

3.8.3 Action 6.3: Identify interesting findings

The next step is to extract interesting findings, such as key findings regarding demand, supply, relevant trends, gaps, dependencies, cybersecurity risks posed by certain categories of products with digital elements (for which sweeps may be organised) or anomalies that could point to critical dynamics of the market segment. These and additional insights may emerge from convergent stakeholder views, quantitative trends or outlier opinions that challenge conventional assumptions.

In the short configuration, the identification of findings is streamlined, with emphasis placed on detecting high-level trends and recurring insights that can inform preliminary market characterisation.

In the long configuration, the analysis uncovers nuanced trends, complex correlations and emerging signals that may not be immediately apparent, supported by iterative review cycles and consultations to interpret less straightforward findings.

3.8.4 Action 6.4: Compare views (where applicable)

Finally, the data are reviewed for consistency across stakeholder groups or evidence bases (through cross-validation against other available datasets). If significant divergence is apparent (e.g. due to differing motivations, technical assumptions or policy perspectives), these are highlighted, contextualised and documented. If no major divergence is observed, the analysis proceeds directly to the integration of results. Comparisons of views can mainly be conducted when identical questions are posed to more than one stakeholder category. Such comparisons are very good instruments for highlighting diverse perceptions of similar topics, thus identifying points of action for establishing a balanced view of stakeholders' perspectives'. This can be key to improving the market uptake of products and services, along with promoting their cybersecurity and market maturity.

In the short configuration, the comparison of views is typically limited to identifying and noting clear alignments or diverse views, ensuring that different perspectives are flagged.

In the long configuration, greater attention is paid to understanding the underlying causes of divergence, which may involve contacting the stakeholders for clarification or conducting targeted secondary research to contextualise opposing viewpoints.

3.8.5 Validation

A check is conducted upon completion of the data analysis phase to ensure that the processed data, findings and interpretations are coherent, reliable and aligned with the objectives of the analysis. Validation aims to ensure the consistency of the data and adequate representation.

In the short configuration, this validation is performed internally, with a focus on ensuring that the insights are substantiated and actionable within the available evidence base.

In the long configuration, the validation process may extend to external peer review to test the credibility and applicability of the insights generated, particularly when the analysis reveals contentious or unexpected findings.

3.8.6 Prepare for follow-ups

This step concludes with preparation for any necessary follow-up measures that may arise from the data analysis phase.

In the short configuration, follow-ups are typically limited to noting any outstanding questions or inconsistencies in data that could inform future studies.

In the long configuration, a more structured approach is established, which may include planning additional rounds of data collection, scheduling follow-up consultations with stakeholders to clarify specific insights or designing supplementary analytical exercises to address gaps or uncertainties identified.

3.8.7 Annexes relevant to Step 6

- Annex K – Data Collection
- Annex M – Coding Schemas
- Annex P – Practical Checklists for Analysts

3.9 Step 7: Present and Disseminate the Results (Planned)

The final step involves consolidating the findings and ensuring that they can be communicated effectively to relevant stakeholders. This step also supports the internal learning process and future reuse of data, completing the market analysis cycle with reflection and strategic knowledge transfer.

The actions in this step are listed below and then described right after:

- Action 7.1 – Produce the analysis report;
- Action 7.2 – Visualise key takeaways (where applicable);
- Action 7.3 – Disseminate the results (where applicable);
- Action 7.4 – Assess the effectiveness of the dissemination Activities (where applicable);
- Action 7.5 – Transfer knowledge (where applicable);
- Action 7.6 – Collect lessons learned.

3.9.1 Action 7.1: Produce the analysis report

The first action is to draft the main report. This document should present the aim and scope of the analysis, the methods used, and the findings identified and their implications (see Annex N ‘Example Table of Contents for Market Analysis Report’). If the findings have passed internal quality control, a conclusion and technical annexes are added to the report. Otherwise, quality control loops are implemented before the report can be completed.

In the short configuration, the report is typically concise, and annexes are limited to providing essential supporting evidence. The executive summary is designed for immediate dissemination.

In the long configuration, the report is more comprehensive, including in-depth methodological details, extended discussions of findings and tailored sections addressing diverse stakeholder interests. Multiple iterations of internal review may be included to ensure depth and precision before finalisation.

3.9.2 Action 7.2: Visualise key takeaways (where applicable)

This step consists of creating, where needed, visual elements (graphs, charts, infographics) (see Annex O ‘Examples of Report Infographics) to enhance readers’ understanding of the main messages. If visualisation is deemed unnecessary, the analysis proceeds directly to dissemination. It is advisable to ensure consistency in the look and feel of the visual elements to enhance the readability of results.

In the short configuration, visualisations typically include a limited number of high-impact graphs that distil the core findings.

In the long configuration, the visualisation effort is more elaborate, incorporating custom-designed infographics.

3.9.3 Action 7.3: Disseminate the results (where applicable)

Where appropriate, the report – including graphically prepared overviews of the results – is shared with external stakeholders. If external dissemination is required, the scope and channels are clearly defined. If not, results are dissemination only to internal stakeholders and the process moves on.

In the short configuration, dissemination is usually direct and narrowly focused, conducted only through straightforward channels.

In the long configuration, dissemination strategies are broader and more diverse, potentially including presentations, webinars or targeted briefings tailored to different stakeholder groups.

3.9.4 Action 7.4: Assess the effectiveness of the dissemination activities (where applicable)

The team then evaluates whether the findings have reached their intended audience and have had the desired impact, for instance through key performance indicators. If monitoring the effectiveness of dissemination is deemed necessary, appropriate feedback tools are deployed.

In the short configuration, dissemination is typically assessed informally, based on immediate feedback from close stakeholders.

In the long configuration, a more structured evaluation may be conducted, involving the deployment of evaluation surveys, the collection of user feedback, and the measurement of clicks/downloads, when applicable.

3.9.5 Action 7.5: Transfer knowledge (where applicable)

If internal stakeholders, partners or future analyses could benefit from the findings, structured templates and walk-throughs are prepared and shared. This ensures institutional memory and facilitates knowledge reuse.

In the short configuration, knowledge transfer may consist of brief internal debriefs or annotated documentation.

In the long configuration, knowledge transfer can be more formalised, involving walk-throughs, dedicated training sessions for relevant units and the production of reusable templates or guidelines to inform future analyses.

3.9.6 Action 7.6: Collect lessons learned

Finally, the process concludes with the identification of key lessons learned, in terms of both what worked and what could be improved. Annex Q (‘Template for Documenting Lessons Learned’) can support the completion of this action.

In the short configuration, lessons learned are typically gathered informally, often through internal team reflections or post-process notes.

In the long configuration, a formal exercise to generate lessons learned may involve holding structured workshops, collecting feedback from stakeholders and the production of a dedicated report to capture insights that could be used to refine the ECSMAF methodology or its application in subsequent cycles.

3.9.7 Validation

A final check is conducted after dissemination and knowledge transfer to ensure that all outputs meet the expected standards in terms of quality, relevance and strategic alignment.

In the short configuration, this final review is internal, confirming that deliverables have been shared appropriately and that documentation is complete.

In the long configuration, validation may also involve an external review of outputs or formal sign-off by relevant ENISA governance structures, especially when the findings are intended to inform high-stakes policy or public discourse.

3.9.8 Prepare for follow-ups

Upon the conclusion of the analysis, the team prepares for follow-up measures that may be required, based on stakeholder feedback or emerging trends identified during the analysis.

In the short configuration, follow-up preparation may be limited to noting recommendations for future analyses.

In the long configuration, a structured follow-up roadmap may be developed, identifying potential areas for deeper investigation, opportunities for further stakeholder engagement and mechanisms for refreshing or updating the analysis as new data become available or market conditions evolve.

3.9.9 Annexes relevant to Step 7

- Annex N – Example Table of Contents for Market Analysis Report
- Annex P – Practical Checklists for Analysts
- Annex Q – Template for Documenting Lessons Learned

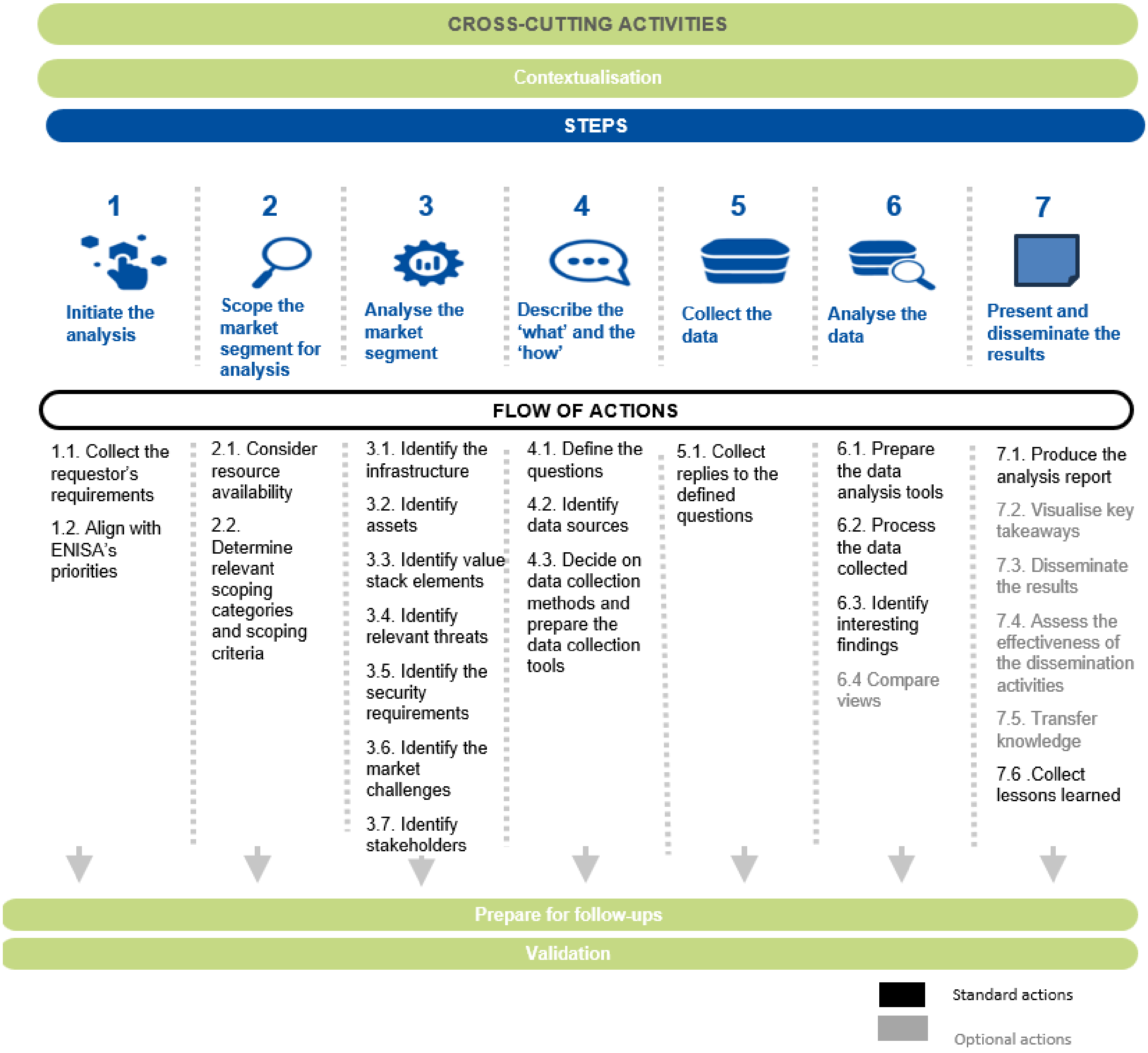
4. Analyses Following Ad hoc Requests (Short and Long Duration)

Analyses following ad hoc requests, also referred to as ‘ad hoc analyses’, are initiated in response to specific needs expressed by stakeholders or highlighted by cybersecurity incidents and events. These analyses can also be short or long in duration, depending on time constraints, urgency, and the scope and depth required.

A short ad hoc analysis is designed to provide rapid, targeted insights using existing data with reduced stakeholder engagement, whereas a long analysis allows for a more thorough investigation, including broader consultation with stakeholders, more in-depth validation and more granular findings.

This chapter describes the steps involved in market analyses following ad hoc requests. In order to increase the readability and the usability of the framework, instead of referring back to parts of the previous chapter (on planned analyses), a full description of each step and action that should be taken during analyses following ad hoc requests is provide, even if this creates redundancy. An overview of the ad hoc steps and actions is provided in **Figure 5**.

Figure 5: Overview of steps and actions involved in analyses following ad hoc requests


CROSS-CUTTING ACTIVITIES
Contextualisation
STEPS
1
Initiate the analysis
2
Scope the market segment for analysis
3
Analyse the market segment
4
Describe the 'what' and the 'how'
5
Collect the data
6
Analyse the data
7
Present and disseminate the results
FLOW OF ACTIONS
1.1. Collect the requestor's requirements
1.2. Align with ENISA's priorities
2.1. Consider resource availability
2.2. Determine relevant scoping categories and scoping criteria
3.1. Identify the infrastructure
3.2. Identify assets
3.3. Identify value stack elements
3.4. Identify relevant threats
3.5. Identify the security requirements
3.6. Identify the market challenges
3.7. Identify stakeholders
4.1. Define the questions
4.2. Identify data sources
4.3. Decide on data collection methods and prepare the data collection tools
5.1. Collect replies to the defined questions
6.1. Prepare the data analysis tools
6.2. Process the data collected
6.3. Identify interesting findings
6.4 Compare views
7.1. Produce the analysis report
7.2. Visualise key takeaways
7.3. Disseminate the results
7.4. Assess the effectiveness of the dissemination activities
7.5. Transfer knowledge
7.6 .Collect lessons learned
Prepare for follow-ups
Validation
Standard actions
Optional actions

4.1 Distinction between Short and Long Duration of Analyses Following Ad hoc Requests

This pathway is relevant to unplanned analyses. Analyses following ad hoc requests are conducted in response to specific needs expressed by stakeholders, or in line with institutional priorities. They can be either short or long in duration depending on the level of effort they require, time constraints and their intended output.

In principle, short- and long-duration ad hoc analyses share the same number of actions. The difference lies mainly in the effort invested for those activities.

A short ad hoc analysis is typically reactive and fast-tracked: it leverages existing data and predefined scoping categories, avoids time-consuming stakeholder engagement and culminates in a concise output. Conversely, a long ad hoc analysis involves a deeper and broader focus on steps such as segment scoping, stakeholder consultation, triangulated validation and the production of results as a comprehensive deliverable. The distinction lies not in the analytical rigour or quality per se, but in the level of iteration, stakeholder involvement and complexity of data visualisation requested, due to time constraints.

Differences in the time allocated to steps in short- and long-duration analyses are shown in figures of the chapter ‘Overview of the Framework’: while **Figure 2** provides indicative durations for each step, **Figure 3** shows differences in the times allocated for short and long ad hoc analyses.

4.2 Recurrent and Continuous Market Monitoring in Analyses Following Ad Hoc Requests

An analysis following an ad hoc request may be a one-off or recurrent. In other words, it may be repeated over time if requested. In addition, in the context of analyses following ad hoc requests, continuous market monitoring can be envisaged.

Recurrence and continuous monitoring are addressed in the chapter ‘Towards Market Analysis Continuity: Recurrent Analyses and Continuous Market Monitoring’.

4.3 Step 1: Initiate the Analysis (Ad Hoc Request)

The first step of an analysis following an ad hoc request is to initiate the analysis by capturing as much information from the requestor as necessary (e.g. requirements of the analysis, stakeholders). The alignment of the request with ENISA’s strategic priorities is assessed. This phase sets the foundation for scoping and ensures the relevance, feasibility and coherence of the analysis.

The actions involved in this step are listed below and described in the sections that follow:

- Action 1.1 – Collect the requestor’s requirements;
- Action 1.2 – Ensure alignment with ENISA’s priorities.

4.3.1 Action 1.1: Collect the requestor’s requirements

The analysis begins with a review of the request submitted, conducted using a template (see Annex C ‘Request Template’). The request is examined to determine various parameters, such as the target market segment, the intended focus of the analysis, the question(s) the analysis is expected to answer, relevant contextual elements (e.g. legal and policy frameworks), the expected time span of the analysis and any preferences indicated with regard to the data collection methodology. Information from the requestor on the intended use of the analysis (e.g. to determine funding priorities, to assess regulatory actions/impact) is relevant. The objective at this stage is to assess whether the request contains all the necessary information and is sufficiently structured to enable a feasible and focused analytical process.

If the request is clear and contains all the necessary information, then the analyst can proceed to Action 1.2 (Ensure alignment with ENISA’s priorities). Otherwise, the following steps are taken.

- **If the request is vague or lacks technical specificity**, an internal clarification loop is triggered, involving engagement with the requestor to refine the input. The revised request is then reassessed.
- **If the request is overly narrow** (e.g. centred on a niche technology or isolated stakeholder group), a scoping exercise is undertaken, followed by a reassessment of the request.
- **If the request spans multiple domains or issues**, it is broken down into sub-requests. Each is triaged against ENISA’s internal categorisations, and the scope of the analysis is iteratively refined in coordination with the requestor. The request is then reassessed.

Once the request is clear and contains all the necessary information, the analyst can proceed to Action 1.2Ensure alignment with ENISA's priorities.

While the rationale of this step is the same, there are some differences between the short and long configurations.

In the short configuration, the assessment of the request and any necessary clarifications are typically addressed in a single interaction with the requestor, ensuring minimal iterations to expedite the process.

In contrast, **the long configuration** allows for multiple exchanges with the requestor and, where necessary, the involvement of internal or external subject matter experts to assist in refining complex or multidimensional requests.

4.3.2 Action 1.2: Ensure alignment with ENISA's priorities

Once the request is deemed sufficiently complete and structured, the next step is to assess whether it aligns with ENISA's strategic objectives and ongoing work priorities. This includes evaluating whether the request is aligned with the Agency's mission, whether it fits within current thematic areas of focus and whether it contributes to the evidence base needed to inform EU cybersecurity policy.

A conditional check is conducted, focused on timing and resource feasibility. If the urgency of the request is compatible with ENISA's planning cycles and available resources, the analysis proceeds to the scoping stage (Step 2). If a conflict arises (e.g. a highly urgent request that cannot be realistically addressed with current capacity) the requestor and ENISA management are consulted find possible ways to accommodate the request (e.g. by deploying additional resources, re-assessing ENISA priorities, modifying the planning). Once an agreement is reached, the alignment check is repeated before moving forward.

This alignment process also varies between the short and long configurations.

In the short configuration, alignment checks are designed to be conclusive within a narrow window to maintain the viability of the analysis.

The long configuration, however, accommodates a more thorough verification of alignment, including cross-referencing against ENISA's annual priorities, coordination with relevant internal units and validation through expert consultation when strategic sensitivities are involved.

4.3.3 Validation

At the end of Step 1, a check is conducted to ensure that the initial request and its alignment with ENISA's priorities have been adequately verified.

In the short configuration, this validation is typically internal, involving rapid cross-checking against priority criteria by the core analysis team.

In the long configuration, the validation step may include consultations with additional internal and external stakeholders or strategic advisors to confirm the coherence and strategic value of proceeding with the analysis.

4.3.4 Prepare for follow-ups

This step also sets the stage for potential follow-up measures: the initial request, any clarifications made and the rationale for alignment decisions are systematically recorded.

This ensures that, if new priorities emerge or if the analysis is revisited in future cycles, the foundational decisions and justifications are transparent and traceable, even **in the short configuration**.

In the long configuration, additional follow-up mechanisms may be established, including the provisional scheduling of interim checks with the requestor or relevant ENISA units.

4.3.5 Annexes relevant to Step 1

- Annex C – Request Template
- Annex P – Practical Checklists for Analysts

4.4 Step 2: Scope the Market Segment for Analysis (Ad Hoc Request)

Once the requestor's requirements have been collected and aligned with ENISA's priorities, the analyst scopes the market segment. This step ensures that the focus of the analysis is both feasible and analytically robust, given available resources and stakeholder expectations.

The actions involved in this step are listed below and described in the sections that follow:

- Action 2.2 – Consider resource availability;
- Action 2.3 – Determine relevant scoping categories and scoping criteria.

4.4.1 Action 2.1: Consider resource availability

The analyst begins by assessing the practical constraints of the analysis, including available time, internal expertise, and the ability to engage relevant stakeholders. These factors are used to calibrate the expected depth and breadth of the study, ensuring that the scope is realistic given operational capacities. A conditional check is performed to determine whether the proposed analysis is comparable to any previous analysis. If the scope and analytical context align with past efforts, underlying assumptions regarding resource needs can be reused with minimal adjustment. In such cases, the process continues directly to defining the scope. However, if the analysis is framed around a familiar topic but the targets of the analysis are different, resource planning will be adapted accordingly.

The assessment of resources focuses strictly on what is required to meet the specific request, without extending to broader strategic considerations. The level of depth applied to the resource assessment depends on whether the configuration is short or long.

In the short configuration, the assessment is confined to internal expertise and existing data sources, avoiding any new capacity building or external consultations. It is important to check with the requestor whether they can make useful resources and data sources available for the analysis.

In the long configuration, a more deliberate assessment is conducted to address novel or complex analytical needs, including consultations within ENISA and/or with external experts, although always proportionate to the scope defined by the request and the requestor's requirements.

4.4.2 Action 2.2: Determine relevant scoping categories and scoping criteria

With resource considerations in place, the next task is to define the analytical framing of the market analysis. This involves selecting the appropriate scoping categories (see Annex E 'Criteria for Scoping the Market Analysis') and criteria that will structure the forthcoming analysis.

The scoping categories selected and their adaptation are determined by the immediate analytical needs highlighted by the request.

A conditional check is then conducted to verify whether the existing ECSMAF scoping categories are sufficient to accommodate the goal of the analysis as issued in the ad hoc request. If they are, the analysis proceeds to the next step (Step 3 Analyse the Market Segment). If the market segment necessitates minor adaptations to the framing (e.g. the reordering of criteria or introduction of a new thematic emphasis), these changes are made while clearly documenting deviation from the standard configuration. Once the revised categories are defined, the analyst proceeds to the next phase.

In the short configuration, the standard ECSMAF scoping criteria (as listed in the Annex E) are applied with as minimal adaptation as possible, unless the requestor specifically asks for comparable material to be used.

In the long configuration, the analyst may adapt the taxonomies to better fit the nuances of the request, but the process remains internally driven based on the request and is not subject to extended rounds of validation.

4.4.3 Validation

At the conclusion of Step 2, a check is conducted to confirm that the resource plan and the selected scoping categories are coherent, sufficient and aligned with the goal of the analysis following the ad hoc request and with ENISA's priorities.

Validation remains internal in ad hoc analyses but is scaled based on the configuration.

In the short configuration, validation is limited to a basic plausibility check by the core team.

In the long configuration, it may involve additional internal reviews or brief expert feedback regarding the scoping criteria, particularly if they have been significantly adapted.

4.4.4 Prepare for follow-ups

Follow-up preparation is proportionate to the depth of the analysis. Any useful experience gained throughout interacting with the requestor is documented for future use.

In the short configuration, follow-ups are limited to internal notes.

In the long configuration, a brief record of potential data gaps or future scoping options is maintained and passed on to the requestor for future consideration.

4.4.5 Annexes relevant to Step 2

- Annex E – Criteria for Scoping the Market Analysis
- Annex P – Practical Checklists for Analysts

4.5 Step 3: Analyse the Market Segment (Ad Hoc Request)

With the scope defined and validated, the analysis moves on to characterising the selected market segment.

In Step 3, the aim is to develop a grounded and structured understanding of the segment. The process follows a logical sequence of investigative actions, each designed to feed into a coherent market profile. The market segment is analysed based on the data already available. It can then be refined, as appropriate, based on additional data that will be collected under Step 5.

In analyses following ad hoc requests, Step 3 follows the same sequence of analytical actions as in the planned analysis pathway. The key difference lies in the degree of tailoring and formalisation, which depends on the specific request and the configuration of the analysis (short or long).

The actions involved in this step are listed below and described in the sections that follow:

- Action 3.1 – Identify the infrastructure;
- Action 3.2 – Identify assets;
- Action 3.3 – Identify value stack elements;
- Action 3.4 – Identify relevant threats;
- Action 3.5 – Identify the security requirements;
- Action 3.6 – Identify the market challenges;
- Action 3.7 – Identify stakeholders.

4.5.1 Action 3.1: Identify the infrastructure

The first analytical task is to map the infrastructure (see Annex F 'Infrastructure Mapping') underpinning the selected market segment. This includes the technical components, systems, platforms, services offered and operational environments that define the segment's architecture. If the required information is readily available (either through existing studies, stakeholder inputs or documentation provided by the requestor) the infrastructure is directly mapped. In the absence of reliable data, a new infrastructure map is developed based on the defined scope. This map serves as the backbone for subsequent asset identification.

In analyses following ad hoc requests, infrastructure mapping (see Annex F 'Infrastructure Mapping') may be simplified, for example when the focus is narrow or when the segment is well known.

In the short configuration, the mapping is developed from existing studies, prior mappings or input provided by the requestor', without introducing any additional infrastructural details, unless strictly necessary.

In the long configuration, infrastructure mapping can be deepened, including primary data collection or expert engagement, where appropriate. The level of detail depends on the specific analytical needs defined in the request.

4.5.2 Action 3.2: Identify assets

Following infrastructure mapping, the analysis identifies key assets that enable or support the functioning of the segment and value creation within it. These may include products with digital elements, digital services, or human capital. The assets identified can be cross-validated by the appropriate stakeholders, depending on the timeline of the analysis. If agreement is not reached, expert triangulation is used to refine the asset list before proceeding.

When addressing the infrastructure of products with digital elements (categorised as important or critical products in accordance with Annex III (Important products with digital elements) and Annex IV (Critical products with digital elements) of the CRA ([33])), parts that could be considered assets have to be identified.

In market analyses following ad hoc requests, asset identification is driven by the level of granularity required by the requestor.

In the short configuration, assets are identified through internal research, focusing on those most central to the segment's functioning.

[33] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj) (accessed 11/03/2026).

In the long configuration, the process can include structured classifications and expert and/or stakeholder input, although the scope should remain proportionate to the depth sought in the request.

4.5.3 Action 3.3: Identify value stack elements

The value stack analysis outlines the layered structure of the collection of services contributing to the value proposition of an organisation. The value stack bundles different products, services, processes or value streams (see Annex B 'Glossary') to increase the overall perceived value for a customer or user. This structured breakdown helps highlight interdependencies and areas of added value. When the structure of the value chain is already defined or recognised, it is documented directly. If the structure is ambiguous or fragmented, expert input or proxy indicators are used to reconstruct it.

The value stack (see Annex G 'Examples of Cybersecurity Value Stacks') is analysed to the extent necessary to achieve the objective of the ad hoc request.

In the short configuration, existing models or prior frameworks are used directly, avoiding the reconstruction of the value stack.

In the long configuration, a deeper investigation can be conducted, for example involving expert consultations or the use of proxy indicators to capture the layered structure of the market segment.

4.5.4 Action 3.4: Identify relevant threats

Through this action, the threat landscape pertinent to the infrastructure being analysed is assessed. Where the segment is linked to critical sectors or regulatory designations (e.g. critical infrastructure under NIS 2 Directive ([34]), products considered critical under the CRA ([35])), the threat list is expanded to include both high-impact and low-probability scenarios. If no specific scoping conditions apply, threats are mapped to include cyber and non-cyber threats in the structure of the assessment.

The approach to threat identification should align with the requestor's needs, along with the impact a threat exposure may have on the assets of the segment under analysis.

In the short configuration, the threat landscape is described using available taxonomies, focusing on established threats.

In the long configuration, threat modelling may be expanded to include more differentiated scenarios or hybrid threat perspectives, when aligned with the objectives defined by the requestor.

4.5.5 Action 3.5: Identify the security requirements

This action focuses on establishing cybersecurity requirements imposed by the infrastructure.

If stakeholders have already adopted a recognised baseline fulfilling these requirements, it is documented and incorporated in the analysis. Moreover, depending on the scope of the analysis, it should consider requirements addressed in emerging, community-driven standards and compliance toolkits developed by standardisation bodies (e.g. open-source stewardship bodies) ([36]).

([34]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27) (accessed 22 July 2025).

([35]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj) (accessed 22/05/2025).

([36]) For example, the EU-funded Eclipse Foundation OCCTET project, the Open Source Security Foundation's Linux Foundation Express Learning 1001 course, and specifications from the Eclipse Open Regulatory Compliance Working Group.

Where comparable past analyses exist, requirements and controls from analogous segments may be reused. The identification of cybersecurity requirements depends on how comprehensive the ad hoc request is.

If the requestor has already identified requirements and a baseline, they are documented. Where comparable previous analyses of requirements exist, they may be reused. In novel cases, secondary data are used to derive a provisional list of security requirements, which is then validated through expert engagement or stakeholder consultation.

In the short configuration, security requirements are identified based on existing standards or prior ENISA outputs.

In the long configuration, bespoke security requirements can be identified and validated with experts or stakeholders when necessary.

4.5.6 Action 3.6: Identify the market challenges

Market challenges are then assessed to identify systemic or operational barriers affecting the segment. Market challenges (see Annex I 'Barriers and challenges') are mapped based on the depth of analysis specified in the request.

Systemic or operational barriers affecting the segment may relate to fragmentation, lack of incentives, barriers to market entry, skills shortages, regulatory gaps, sectoral maturity (if applicable), technological immaturity (as established by the technology and innovation radar ([37])), cybersecurity risks (indicated, for example, by market trends or consumer complaints) ([38]), innovation gaps, etc. Where known challenges exist, they are clustered by type and market impact. If no challenges are evident or the information is unavailable, the analysis proceeds directly to stakeholder mapping.

In the short configuration, challenges are identified through desk research and familiar data.

In the long configuration, additional expert inputs or simple analytical frameworks can be used to prioritise or classify systemic barriers.

4.5.7 Action 3.7: Identify stakeholders

The final action of Step 3 (Analyse the Market Segment) maps those involved in or affected by the market segment.

Stakeholder mapping in analyses following ad hoc requests is proportionate to the analytical scope agreed with the requestor.

This mapping typically includes supply-side and demand-side stakeholders, regulatory bodies, and research and development institutions.

When identifying stakeholders, special attention should be given to start-ups and scale-ups, since they play an important role in innovation.

If stakeholders' roles and relationships are already clear, they are mapped directly. If they are not, stakeholder groups are categorised using structured tools such as power–interest matrices, ensuring that their roles are adequately captured to facilitate subsequent engagement.

In the short configuration, mapping is focused on key institutional and market actors.

([37]) See ENISA's technology and innovation radar methodology (to be published).

([38]) The biennial technical report on emerging cybersecurity risks, which ENISA is tasked with preparing under the CRA (see Art. A17, para. 3 and Recital 69), is an important document to consider when addressing the cybersecurity risks.

In the long configuration, the mapping may be expanded to include emerging actors and is supported by categorisation tools if relevant.

4.5.8 Validation

At the conclusion of Step 3, a check is conducted to ensure the completeness and accuracy of market segment characterisation.

In ad hoc analyses, validation is adapted to the configuration.

In the short configuration, validation is conducted internally with optional expert checks if relevant data are available or sufficient expertise is available.

In the long configuration, validation includes structured feedback from relevant experts or internal units, and ensuring alignment with what was explicitly agreed with the requestor.

4.5.9 Prepare for follow-ups

This step concludes with the preparation for follow-up measures, particularly regarding any data gaps identified, contested findings, areas requiring further investigation, and continuing the analysis, where appropriate, jointly with the requestor. Moreover, new threats or requirements or any other related information is added to the internal knowledge base.

In the short configuration, follow-ups are noted as recommendations or optional areas for future exploration for the requestor.

In the long configuration, a basic plan for potential follow-up measures is outlined, capturing any data gaps, emerging questions, or additional analytical dimensions that could be addressed in future cycles or related studies.

4.5.10 Annexes relevant to Step 3

- Annex B – Glossary
- Annex F – Infrastructure Mapping
- Annex G – Examples of Cybersecurity Value Stacks
- Annex H – Stakeholders
- Annex I – Barriers and Challenges
- Annex J – Methodology
- Annex P – Practical Checklists for Analysts

4.6 Step 4: Describe the ‘What’ and the ‘How’ (Ad Hoc Request)

With the analytical scope in place, Step 4 involves defining the guiding questions, identifying relevant data sources and selecting appropriate data collection methods. The goal of this step is to ensure that the forthcoming data collection and related stakeholder engagement are targeted, relevant and adapted to the analysis context.

In analyses following ad hoc requests, preparation for stakeholder engagement involves the same sequence of actions as in planned analyses.

The level of customisation and formalisation is adjusted based on the specific requirements of the request and the selected configuration (short or long).

The actions involved in this step are listed below and described in the sections that follow:

- Action 4.1 – Define the questions;
- Action 4.2 – Identify data sources;
- Action 4.3 – Decide on data collection methods and prepare the data collection tools.

4.6.1 Action 4.1: Define the questions

The analyst begins by formulating a set of questions, based on the input received in Step 1 from the requestor and on the resources available.

In analyses following ad hoc requests, the formulation of guiding questions (see Annex L 'Examples of Survey Questions for Each Stakeholder Type') is shaped directly by the requestor's priorities, the resources available and the analytical scope established in previous steps.

The questions should reflect the specific scope of the analysis and be calibrated to the types of stakeholders involved. If requestor priorities, scope and stakeholders are comparable to a previous ENISA market analysis, the same questions can be reused or adapted. If the scope is different, the existing questions should be reprioritised and modified. If new stakeholders are involved, additional questions are incorporated. Where both the scope and the stakeholder landscape differ significantly, a full overhaul of the question set is required.

In the short configuration, predefined or previously used question sets are applied with minimal adjustment unless new stakeholder types are involved.

In the long configuration, the question set can be tailored to reflect new elements of the scope or stakeholder perspectives, though the extent of redesign depends on the specificity of the request rather than on broader exploratory aims.

4.6.2 Action 4.2: Identify data sources

Once the questions are decided, the analyst identifies where the data to answer them can be found, and compiles a list of data sources (see Annex J 'Methodology') to support the analysis. The mapping of data sources in ad hoc analyses is proportionate to the scope of the analysis and the availability of information.

Data sources may include previous ENISA studies, academic literature, regulatory documents, official statistical repositories, proprietary datasets, expert contacts and sector-specific insights.

Mapping data sources at this stage helps structure stakeholder engagement and ensures that stakeholders' inputs complement rather than duplicate existing evidence.

When mapping the data sources, analysts should consider whether the data are provided on a voluntary basis or as part of a structured mandatory reporting mechanism, and whether they are provided on an ad hoc basis or on a regularly basis.

In the short configuration, the analyst focuses on immediately available, validated and accessible data sources that are directly applicable to the request.

In the long configuration, a broader set of sources may be mapped, including less formal or emerging datasets; however, the mapping remains focused on the analytical objectives, not including comprehensive data unless explicitly requested.

4.6.3 Action 4.3: Decide on data collection methods and prepare the data collection tools

The final preparatory action involves selecting data collection methods and designing the appropriate tools. The choice of data collection methods and tools (see Annex K 'Data collection') in ad hoc analyses is directly influenced by the deliverable to be produced, the engagement expectations set by the requestor and the timeline.

Where extensive engagement is required and feasible, a detailed survey is deployed. If time is more constrained, focused interviews or moderated workshops are organised. Where limited engagement is anticipated, leaner approaches using publicly available data or data already available from other sources (including data collected by ENISA or available from other external sources), brief surveys and expert validation rounds are to be adopted. The methods selected are then operationalised through well-designed instruments aligned with the scope and questions defined earlier.

When deciding on data collection methods and preparing the relevant tools, it is important to put in place measures to ensure triangulation, bias mitigation and data quality.

In the short configuration, the analyst selects straightforward methods, often adapting existing templates for surveys or interviews to minimise preparation time and complexity.

In the long configuration, method selection is more versatile, and processes may include a combination of data collection techniques.

4.6.4 Validation

Step 4 concludes with a check aimed at ensuring the consistency and quality of the data, but also adequate representation. Moreover, it ensures the robustness of analysis design and alignment with both the scope of the analysis and the analytical objectives of the requestor.

The validation of the design for engaging stakeholders in ad hoc analyses is scaled based on the configuration.

In the short configuration, validation is internal, ensuring coherence with the scope and resource plan, without formal stakeholder input.

In the long configuration, validation can involve targeted feedback from selected experts or internal reviewers, especially when methods or question sets have been customised beyond standard practice.

4.6.5 Prepare for follow-ups

This step includes preparatory actions for potential follow-up measures.

In the short configuration, preparatory notes on potential engagement gaps or anticipated limitations are briefly recorded, but no structured follow-up mechanisms are formalised.

In the long configuration, a simple follow-up plan may be established, outlining possible re-engagement with stakeholders, further rounds of data collection or alternative engagement strategies, particularly if the analysis anticipates varied stakeholder response rates or complex data needs.

4.6.6 Annexes relevant to Step 4

- Annex B – Glossary
- Annex J – Methodology
- Annex K – Data Collection
- Annex L – Examples of Survey Questions for Each Stakeholder Type
- Annex P – Practical Checklists for Analysts

4.7 Step 5: Collect the Data (Ad Hoc Request)

With the data sources and data collection methods identified and the relevant tools prepared (e.g. the EU Survey tool), the analysis proceeds to data collection. This phase may involve engaging stakeholders directly to capture input on the questions defined during the preparatory stage. The objective is to gather reliable, targeted information that will enrich the desk research and support the development of a robust market analysis.

Market analysts can gather the data they need for their analyses by a variety of means and from a variety of sources. They can conduct either primary or secondary research

- **Primary research** is conducted through surveys, interviews, focus groups and observation. These activities are performed directly by the owner of the market analysis, who is also the data owner. Surveys, interviews and focus groups are examples of primary (or empirical) research.
- **Secondary research** is conducted by collecting data from already available sources, such as online communities, contractors and automated/manual open-source searches. The owner of the market analysis does not own the material collected from secondary research. A literature review is an example of secondary research.

In analyses following ad hoc requests, Step 5 has the same overall structure as in the planned analysis pathway.

The approach to data collection is adapted to the configuration of the analysis (short or long) and the specific requirements of the request.

The action in this step is Action 5.1 (collect replies to the defined questions).

4.7.1 Action 5.1: Collect replies to the defined questions

Stakeholder engagement is carried out using the selected methods. In analyses following ad hoc requests, stakeholder engagement is aligned directly with the scope and depth of analysis agreed in prior steps.

Regardless of the method, the input collected is documented systematically and checked for consistency.

Throughout this phase, it is essential to keep track of the data collection methodology (see Annex K ‘Data collection’) through appropriate documentation. This includes keeping records of the tools used, the selection criteria for stakeholders, formats for stakeholder engagement and any deviations from the planned process.

In parallel, all data collection activities must be conducted in line with appropriate regulations, for example concerning stakeholder engagement, data privacy and intellectual property rights. This entails securing informed consent, ensuring confidentiality where applicable, and aligning the engagement approach with ENISA’s ethical standards and regulatory obligations.

In the short configuration, data collection is based mainly on the use of secondary data (see Annex J ‘Methodology’) and engagement with a focused set of stakeholders, prioritising those most critical to the analysis.

In the long configuration, a wider and more diverse set of stakeholders can be engaged, using a combination of methods such as interviews and focus groups, as appropriate to the objectives of the request. The methodology, along with any deviations from the original plan, is documented more comprehensively but remains tailored to the analytical depth required.

In both configurations, data privacy, informed consent, intellectual property rights and confidentiality continue to apply consistently, in alignment with ENISA's ethical standards.

4.7.2 Validation

The validation of data collection in analyses following ad hoc requests is scaled based on the configuration.

In the short configuration, validation is limited to an internal review by the analysis team, ensuring that responses sufficiently address the guiding questions.

In the long configuration, validation can include sharing a synthesis of responses with selected internal stakeholders (and external experts, where relevant), to confirm the integrity and completeness of the data collected.

4.7.3 Prepare for follow-ups

Data collection concludes with the preparation for potential follow-up measures. At this stage, experience with tool usage and stakeholder responses (including quality and consistency), etc. are documented.

In the short configuration, follow-up measures are informal and focused on clarifying any immediate inconsistencies or gaps identified during the initial data review.

In the long configuration, a more structured follow-up plan is established, outlining the need for additional engagement rounds, targeted data requests or further consultations to resolve any outstanding questions or gaps in the dataset.

4.7.4 Annexes relevant to Step 5

- Annex K – Data Collection
- Annex P – Practical Checklists for Analysts

4.8 Step 6: Analyse the Data (Ad Hoc Request)

Once data collection is complete, the analysis progresses to processing and interpreting the information gathered. This step ensures that the data are made usable through cross-validation across sources, homogenisation and transformation into meaningful insights.

In an analysis following an ad hoc request, the structure of data analysis mirrors the planned analysis pathway.

The tools used, depth of interpretation and validation mechanisms are adapted based on the specific objectives of the request and the configuration chosen.

The actions involved in this step are listed below and described in the sections that follow:

- Action 6.1 – Prepare the data analysis tools;
- Action 6.2 – Process the data collected;
- Action 6.3 – Identify interesting findings;
- Action 6.4 – Compare views (where applicable).

4.8.1 Action 6.1: Prepare the data analysis tools

Before the analysis begins, appropriate data analysis tools must be selected and prepared based on the type of data collected, the time available, the desired depth of insight and the way in which results will be presented. These tools may include structured templates (see Annex K 'Data collection'), qualitative coding schemes (systems for categorising and labelling textual or interview data) (see Annex M 'Coding schemas') or quantitative processing utilities (tools for handling numerical data and performing statistical analysis).

In the short configuration, tools are selected from existing templates or utilities already in use within ENISA, focusing on those that enable efficient processing and data visualisation without the need for extensive customisation.

In the long configuration, the analyst selects or adapts tools that can handle diverse data types and support more sophisticated analysis and visualisation options. The functionalities of the tool remain in line with the specificities of the request rather than advanced purposes.

4.8.2 Action 6.2: Process the data collected

The raw data are then organised, cleaned and structured to facilitate interpretation. This includes removing redundancies, harmonising formats and clustering the information in a way that enables meaningful comparison across sources (see Annex K 'Data Collection').

Data processing in analyses following ad hoc requests remains proportional to the analytical scope (see Annex K 'Data Collection').

In the short configuration, data are standardised and formatted (see Annex B 'Glossary') for direct interpretation, prioritising operational readiness (see Annex B 'Glossary') over methodological depth.

In the long configuration, data processing includes more thorough cleaning, coding (see Annex M 'Coding Schemas') and structuring to enable multidimensional comparisons, though always constrained to the analytical needs established at the outset.

4.8.3 Action 6.3: Identify interesting findings

The next step is to extract interesting findings, such as key findings regarding demand, supply, relevant trends, gaps, dependencies, cybersecurity risks posed by certain categories of products with digital elements (for which sweeps may be organised) or anomalies that could point to critical dynamics of the market segment. These insights may emerge from convergent stakeholder views, quantitative trends or outlier opinions that challenge conventional assumptions.

The extraction of findings in ad hoc analyses is driven by the configuration.

In the short configuration, the focus remains on identifying clear, high-level trends and insights directly relevant to market characterisation.

In the long configuration, the analyst explores more nuanced trends and correlations, potentially involving rounds of internal review or consultation (purposefully scoped to avoid unnecessary breadth beyond the requestor's objectives).

4.8.4 Action 6.4: Compare views (where applicable)

Finally, the data are reviewed for consistency across stakeholder groups or evidence bases (through cross-validation against other available datasets). If significant divergence is apparent (e.g. due to differing motivations, technical assumptions or policy perspectives), these are highlighted, contextualised and documented. If no major divergence is observed, the analysis proceeds directly to the integration of results.

The process of comparing findings across stakeholder inputs or data sources is tailored to the expected depth of the deliverable. Views can be compared with the aim of identifying and noting clear alignments or diverse opinions, ensuring that differentiated perspectives are flagged.

In the short configuration, divergence is flagged and documented but not extensively analysed unless critical to the analysis.

In the long configuration, significant divergence and alignments among stakeholder views are explored in depth, which may involve re-engaging with stakeholders or carrying out targeted secondary research to contextualise opposing perspectives.

4.8.5 Validation

A check is conducted upon completion of the data analysis phase to ensure that the processed data, findings and interpretations are coherent, reliable and aligned with the objectives of the analysis. Validation aims to ensure the consistency of the data and adequate representation.

In the short configuration, validation is performed internally by the core team, ensuring that the findings are plausible and directly usable for the deliverable.

In the long configuration, validation may include seeking expert feedback or carrying out internal cross-review.

4.8.6 Prepare for follow-ups

This step concludes with preparations for any necessary follow-up measures that may arise from the data analysis phase.

In the short configuration, follow-ups are informal, with any unresolved questions or data gaps noted as observations for potential future work.

In the long configuration, a more structured follow-up framework is drafted, identifying possible needs for additional data, further stakeholder consultations or analyses that could enhance the findings in future rounds of analysis or related requests.

4.8.7 Annexes relevant to Step 6

- Annex K – Data Collection
- Annex M – Coding Schemas
- Annex P – Practical Checklists for Analysts

4.9 Step 7: Present and Disseminate the Results (Ad Hoc Request)

This final step involves consolidating the findings and ensuring that they can be effectively communicated to relevant stakeholders. This step also supports internal learning and future reuse of data, completing the market analysis cycle with reflection and strategic knowledge transfer.

In an analysis following an ad hoc request, dissemination involves the same sequence of actions as in the planned analysis pathway.

Scope, formalisation and output are adapted based on the ad hoc request and the configuration of the analysis.

The actions involved in this step are listed below and described in the sections that follow:

- Action 7.1 – Produce the analysis report;

- Action 7.2 – Visualise key takeaways (where applicable);
- Action 7.3 – Disseminate the results (where applicable);
- Action 7.4 – Assess the effectiveness of the dissemination activities (where applicable);
- Action 7.5 – Transfer knowledge (where applicable);
- Action 7.6 – Collect lessons learned.

4.9.1 Action 7.1: Produce the analysis report

The first action is to draft the main report. This document should present the aim and scope of the analysis, the methods used, and the findings identified and their implications (see Annex N 'Example Table of Contents for Market Analysis Report'). If the findings have passed internal quality control, a conclusion and technical annexes are added to the report. Otherwise, quality control loops are implemented before the report can be completed.

In ad hoc analyses, the reporting format (see Annex N Example Table of Contents for Market Analysis Report) is shaped by the specificity and depth required by the configuration option of the request.

In the short configuration, the report remains concise, focusing on essential findings, with a limited number of annexes. The executive summary is designed to enable rapid comprehension and immediate use by the requestor.

In the long configuration, the report can be more extensive, including detailed methodological explanations and tailored sections for diverse stakeholders, but the level of detail remains proportionate to the objectives of the request.

4.9.2 Action 7.2: Visualise key takeaways (where applicable)

This step consists of creating, where needed, visual elements (graphs, charts, infographics) (see Annex O 'Examples of Report Infographics') to enhance understanding of the main messages. If visualisation is deemed unnecessary, the analysis proceeds directly to dissemination. It is advisable to ensure consistency in the look and feel of the visual elements to enhance readability of results.

In the short configuration, visual elements are limited to core graphics (see Annex O 'Examples of Report Infographics') that succinctly represent the main insights, drawing from standard visual templates where available.

In the long configuration, visualisation is more tailored and may include bespoke infographics, but typically remains focused on enhancing stakeholders' understanding within the scope of the specific request.

4.9.3 Action 7.3: Disseminate the results (where applicable)

The process for disseminating results following an ad hoc analysis request aligns directly with the intended audience specified in the request.

In the short configuration, dissemination is direct, using straightforward channels, and is restricted to the requestor and any immediately relevant stakeholders.

In the long configuration, the results may be disseminated to a broader audience, but their distribution is still guided by the requestor's expectations.

4.9.4 Action 7.4: Assess the effectiveness of the dissemination activities (where applicable)

In an analysis following an ad hoc request, the requester usually assesses the effectiveness of dissemination.

In the short configuration, the effectiveness of dissemination is usually gauged through informal feedback from the requestor or stakeholders directly involved in the analysis.

In the long configuration, a more systematic assessment may be implemented, for example collecting targeted feedback or simple usage metrics (clicks/downloads).

4.9.5 Action 7.5: Transfer knowledge (where applicable)

Knowledge transfer in ad hoc analyses is based on the potential for reuse.

In the short configuration, internal knowledge transfer is informal, typically limited to internal notes, briefings, or outputs stored in internal repositories.

In the long configuration, more formal knowledge sharing can be conducted, including documentation templates or dedicated sessions for relevant ENISA teams, especially if the topic is likely to recur or holds broader strategic relevance.

4.9.6 Action 7.6: Collect lessons learned

Finally, the process concludes with the identification of key lessons learned, in terms of both what worked and what could be improved. Annex Q (‘Template for documenting Lesson Learned’) can support the completion of this action.

In the short configuration, lessons learned are captured informally, for example through team debriefs or brief post-analysis reflections.

In the long configuration, lessons learned may be collected from structured feedback from the team and selected stakeholders. These can feed into updates to analytical templates or methods, depending on the complexity of the analysis.

4.9.7 Validation

A final check is conducted after dissemination and knowledge transfer to ensure that all outputs meet the expected standards in terms of quality, relevance and strategic alignment.

Validation after dissemination in ad hoc analyses remains dependent on the configuration.

In the short configuration, final validation takes the form of an internal quality check by the analysis team, to ensure that outputs meet the expectations of the requestor.

In the long configuration, an additional review step can be included (involving either external experts (if the requestor agrees) or internal stakeholders), particularly if the deliverable is sensitive or designed to inform broader institutional priorities.

4.9.8 Prepare for follow-ups

Upon the conclusion of the analysis, the team prepares for follow-up measures that may be required, based on feedback, in particular from the requestor, or emerging trends identified during the analysis.

In the short configuration, follow-up preparation is limited to the compilation of informal notes on areas for potential further enquiry.

In the long configuration, a more structured follow-up roadmap can be established, providing options for deeper investigation, potential stakeholder re-engagement, or updating the analysis if the relevant market segment evolves or a new request is received.

4.9.9 Annexes relevant to Step 7

- Annex N – Example Table of Contents for Market Analysis Report
- Annex P – Practical Checklists for Analysts
- Annex Q – Template for documenting Lesson Learned

5. Towards Market Analysis Continuity: Recurrent Analysis and Continuous Market Monitoring

In the previous chapters we described one-off market analyses (planned and following ad hoc requests). There are, however, circumstances in which market analyses need to be repeated over time (**recurrent analysis**), or even continuously to track market developments over a specific period (**continuous market monitoring**, also referred to simply as ‘market monitoring’).

Cybersecurity market analysis, as covered in this framework (ECSMAF V3.0), is, at its core, a tool for assessing various cybersecurity market characteristics: it provides the means to set up, scope and perform a cybersecurity market analysis, while taking into account various flexibility requirements (e.g. in terms of timeline, depth, breadth and market stakeholders). As a tool per se, this framework does not entail any information regarding the frequency of its use, for example for long-term assessments in a specific product/service segment. The need for the recurrent or continuous use of the analysis tool emerges from the necessity to monitor market-related phenomena that happen across a given time span.

There are various types of events that indicate the potential emergence of a phenomenon with market impact. Some examples of events that may have a market impact are summarised below. They encompass various event types that may affect – directly or indirectly – the demand for and/or the supply of certain cybersecurity products or services.

- **Events regarding technological issues.** Malicious attacks and technical failures of products are the primary events affecting the cybersecurity properties of a product. Such incidents may affect product functionality, thus affecting the acceptance and positioning of a product in the market. In the case of hardware, for example, the existence of vulnerabilities may even lead to withdrawal of products from the market. Other examples of technological issues are non-fulfilment of cybersecurity requirements, weaknesses in the operation of products ([39]), failures through physical events, or the emergence of new technologies (e.g. quantum computing or AI) or threats.

  Given the complexity of (software and hardware) products and their supply chain, technical failures of various, heavily reused modules may affect a large number of products. As an example, one can consider open-source software (OSS): given the high degree of reusability of OSS, weaknesses may affect many products using a vulnerable OSS module and generate a critical market impact.

  When an event is detected, the subsequent analysis should differentiate between (a) vulnerabilities in non-commercial, community-driven projects; (b) vulnerabilities in projects managed by a formal ‘open source software steward’ (e.g. a foundation) with defined vulnerability management processes; and (c) vulnerabilities in commercial OSS components

[39] The Common Weakness Enumeration, which is ‘is a community-developed list of common software and hardware weakness types that could have security ramifications’ (MITRE, ‘New to CWE’, Common Weakness Enumeration website, https://cwe.mitre.org/about/new_to_cwe.html (accessed (17/11/2025) could be a useful reference for identifying weaknesses in hardware, software or service components.

offered by a 'manufacturer' as defined by the CRA. This distinction is critical for correctly assessing market risk and applying a proportionate response.

- **Events regarding process-related issues.** Such events are relevant mainly to offered services. They include weaknesses of service offerings that lead to impactful incidents. Such weaknesses may be caused by human errors, errors in the workflow of a service process, technical failures of intermediate systems, etc. It is worth mentioning that weaknesses in operational and maintenance processes may cause technological failures, such as violations of access rights, misconfigurations and erroneous updates.

  In organisations with mature risk assessment processes, internal activities are permanently monitored using risk management frameworks, risk registers, etc. When an event is detected, risk assessment and risk management procedures kick in to measure and mitigate potential risks and introduce corrective measures.

- **Events regarding financial issues.** The long-term availability of financial resources is key to the development, maintenance and improvement of products and services, and therefore to the market positioning of products. Besides financial solvency issues, events regarding the finances of an organisation may include the origin of venture capital, the structure of its stakeholders and its financial policy. Structure of stakeholders and flow of capital may be indicative of the origin of company control (e.g. whether it is EU controlled).

  Assuming that entities involved in the finances of a company may exert significant influence in product development and maintenance, it is worth observing the financial structure and financial transactions of companies owning/operating strategic products.

- **Events regarding product- or company-related strategic issues.** A number of issues regarding company-related and/or product-related strategy may be of importance for market positioning and product quality. Some examples (non-exhaustive) are:

  - design decisions regarding the supply chain of a product;
  - the staff acquisition strategy;
  - the subcontracting/outsourcing of parts of product development/operation to other organisations;
  - take-over of a product by another organisation;
  - movement of the headquarters of a company to another country;
  - composition of and changes regarding company management structure and management board.

It is worth mentioning that an event may be a combination of more than one of the above types. For example, a process-related event may result in a technical issue. Conversely, a technical issue may be caused by product- or company-related strategic issues (e.g. product design decisions), finance-related issues or process-related issues. Moreover, it is important to note that the above list of event types is only indicative, with other event types connected to geopolitical issues, natural disasters and the effects of climate change. With further experience in the area of market analysis, and continuous market monitoring in particular, more and more types of events may be added to the list.

The detection of these events may motivate the initiation of a continual market analysis effort in an attempt to assess the market impact over a certain time horizon on product/service segments, for instance in a critical sector (e.g. energy, health).

5.1 Recurrent Market Analysis

Recurrent market analyses generate **snapshots** of market characteristics at discrete time intervals (e.g. monthly, annually) for a specific product/service segment.

Recurrent market analyses involve the repetitive/periodic application of a properly scoped market analysis activity for a specific sector or product category. A recurrent market analysis can be performed in both a planned and an ad hoc manner. A recurrent planned market analysis may be initiated to follow up on market developments in an important emerging technological area (e.g. AI) that has been initially analysed through a planned project. An ad hoc recurrent analysis can be performed in order to assess specific types of market impact caused by events in a specific area (thus having a more specific / narrower scope).

It is possible for certain ad hoc requests to become recurrent, either because the requestor identifies a need for periodic updates or because the underlying topic evolves rapidly. In such cases, the application of the framework adapts accordingly. Recurring requests benefit from the analytical groundwork established in the initial analysis cycle, allowing for the more efficient reuse of scoping categories, stakeholder maps and data collection instruments. This continuity enables the analysis to shift progressively from a purely reactive mode to a semi-structured monitoring exercise. Over time, the level of iteration and validation can be recalibrated to reflect the evolving maturity of the segment under analysis, the increasing familiarity with stakeholder dynamics and the growing availability of longitudinal data. As a result, the methodology may evolve to take on a hybrid format that blends the flexibility of ad hoc responses with the consistency typical of planned analytical cycles.

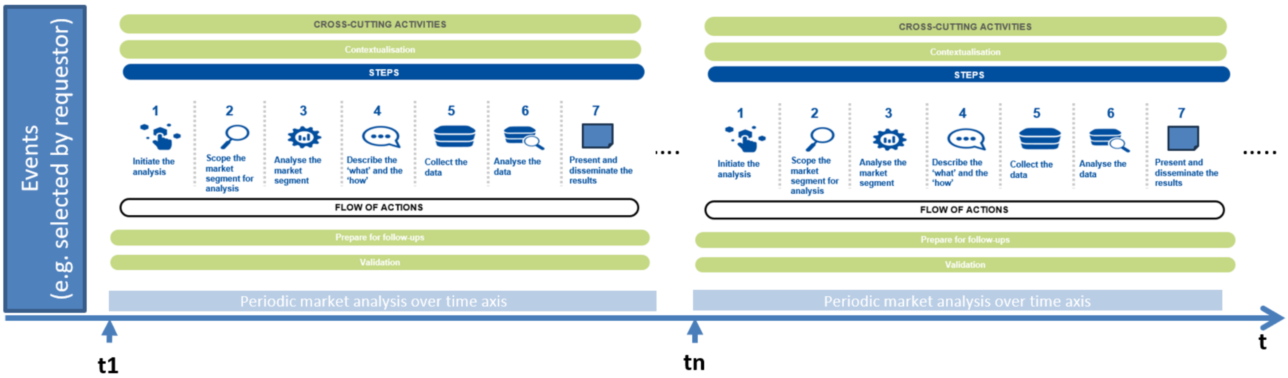
Recurrent analyses leverage previous scoping, data sources and stakeholder networks to ensure continuity and comparability across rounds. This allows ENISA and its stakeholders to monitor market trends, assess changes in threats, technologies and regulatory impacts, and refine analytical approaches based on lessons learned. Recurrence can be planned or triggered by requests connected to events, such as significant policy changes, emerging risks or shifts in market dynamics. To this extent, recurrent market analyses are also preceded by the identification of an event whose market impact is assessed at regular time intervals.

Hence, in recurrent market analyses, a properly scoped analysis (in an identical manner to the one-off analysis), can be performed to create snapshots of a single market segment periodically. Eventually, the scope of the initial analysis may be adapted to cover changing requirements over time. An indicative form of recurrent market analysis is depicted in

Figure 6.

The steps displayed in Figure 6 and Figure 7 are the same as those in the workflow in Figure 1.

Figure 6: Indicative timeline for recurrent market analysis


Events
(e.g. selected by requestor)
CROSS-CUTTING ACTIVITIES
Contextualisation
STEPS
1 Initiate the analysis
2 Scope the market segment for analysis
3 Analyse the market segment
4 Describe the 'what' and the 'how'
5 Collect the data
6 Analyse the data
7 Present and disseminate the results
FLOW OF ACTIONS
Prepare for follow-ups
Validation
Periodic market analysis over time axis
....
CROSS-CUTTING ACTIVITIES
Contextualisation
STEPS
1 Initiate the analysis
2 Scope the market segment for analysis
3 Analyse the market segment
4 Describe the 'what' and the 'how'
5 Collect the data
6 Analyse the data
7 Present and disseminate the results
FLOW OF ACTIONS
Prepare for follow-ups
Validation
Periodic market analysis over time axis
.....
t1
tn
t

Legend:

t: stands for time axis

t1: indicates the start of the first execution

tn: indicates the start of a consecutive execution

5.2 Continuous Market Monitoring

Before addressing continuous market monitoring, let us use the monitoring of system operation as an analogy. In system operation, as opposed to a snapshot (provided by the recurrent/periodic application of an analysis), **continuous monitoring** is a **permanent, (semi-)automated process** of tracking the state of a system (usually based on event detection), with the aim of assessing whether a set of defined rules governing performance is maintained during operation. Based on the data collected, continuous monitoring checks if the system operates in accordance with specified rules. Upon the detection of an **event indicating a violation of those rules**, a continuous monitoring system will flag the event to the operator. Continuous monitoring enables permanent control over a process or system. Once continuous monitoring has generated an alert due to a rule violation, an analysis process is necessary to understand the root cause(s) and identify courses of action to re-establish 'normality'.

In market analysis, continuous market monitoring is a continuous activity used to observe the impact of a phenomenon on the relevant market segment, a typical task performed within market observatories ([40]).

It is worth mentioning that continuous market monitoring is a distinct, stand-alone and **permanent** activity that is related to market analysis: once continuous market monitoring has detected a relevant event (i.e. fulfilling the monitoring rules), a market analysis activity can be initiated to analyse potential consequences of the event for relevant market products. Given the unforeseen nature and the specific focus of an event, the market analysis resulting from its detection will most probably be ad hoc.

Continuous market monitoring is expected to acquire particular importance especially in light of the increasing complexity of the cybersecurity market and the regulatory demands introduced by the CRA. Only through continuous monitoring it is possible, for instance, to detect systemic risks at an early stage, before they escalate, react quickly to changes in products, certifications and vulnerabilities, and spot capability gaps across sectors or product categories as they evolve. Furthermore, continuous market monitoring can support strategic foresight, enabling ENISA and stakeholders to anticipate shifts rather than react to them.

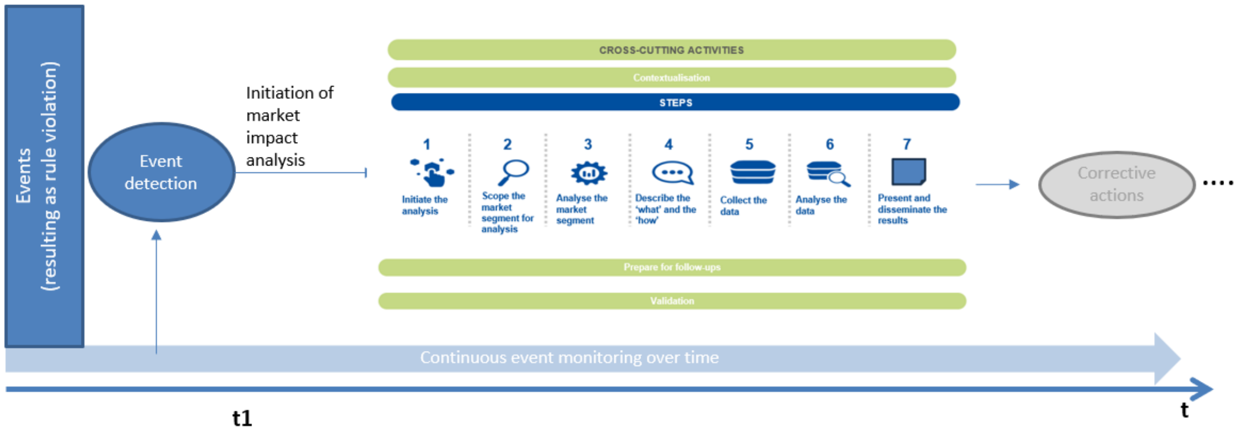
[40] Market observatories are established in various sectors of our economy, for instance agriculture (see Report from the Commission to the European Parliament and the Council on Union market observatories, COM(2023) 679 final of 31 October 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0679).

Continuous cybersecurity market monitoring may be a (semi-)automated activity in which some market events are monitored (e.g. the changing market state of a product (e.g. issuance of a certificate), the takeover of a company, a change in products, the vulnerability of a certified product). Generally speaking, prior to a continuous market monitoring activity, the rules for monitoring – that is, methods for the assessment of root causes, market actions to be taken to respond to the monitored event, etc. – have to be set. Once an event has been detected, a market analysis of the related market may be initiated.

Continuous market monitoring is expected to be gradually established as the implementation of the CRA ([41]) proceeds: important/critical product categories will be better scrutinised through CRA provisions (e.g. requirements, software bills of materials, security controls). In this way, impactful, technical cybersecurity events will be more easily linked to product components. At the same time, with CRA implementation in place, product-related data sources will be available in larger volumes, facilitating more efficient connection between events, product components, vendors and end users.

Continuous market monitoring has interfaces with existing cybersecurity monitoring systems, such as cyber security incident response teams, security operations centres, emergency response and cyber-diplomacy. The interplay with such monitoring systems will be investigated in forthcoming ENISA work. An indicative form of continuous market monitoring is presented in **Figure 7**.

Figure 7: Indicative timeline for continuous market monitoring


Events
(resulting as rule violation)
Event detection
Initiation of market impact analysis
CROSS-CUTTING ACTIVITIES
Contextualisation
STEPS
1
Initiate the analysis
2
Scope the market segment for analysis
3
Analyse the market segment
4
Describe the 'what' and the 'how'
5
Collect the data
6
Analyse the data
7
Present and disseminate the results
Prepare for follow-ups
Validation
Corrective actions
....
Continuous event monitoring over time
t1
t

Legend:

t: stands for time axis

t1: indicates the start of the first execution

5.3 In Summary

Until a certain CRA maturity level is reached, the most frequent types of market analysis are expected to remain one-off (i.e. planned or ad hoc) analyses, and in some cases recurrent analyses. On the detection of an event, a request for an entity (e.g. ENISA or another organisation conducting cybersecurity market analysis) to conduct a market analysis will normally lead to the performance of a one-off, or in some cases a recurrent, market analysis to assess the market impact of the event and identify possible corrective measures. Continuous market monitoring may be performed too when a specific need for it is raised by a concerned stakeholder. Nonetheless, continuous market monitoring

[41] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj) (accessed 22/05/2025).

needs are expected to emerge, when a certain CRA maturity level has been reached through the adoption of CRA provisions by vendors.

ECSMAF is capable of covering a variety of market analysis needs, by providing all components necessary to support different kinds of cybersecurity market analysis (including recurrent market analysis and continuous market monitoring) in various levels of detail.

6. Conclusions

ECSMAF V3.0 provides a practical, rigorous and configurable way to conduct cybersecurity market analyses across a variety of policy and operational contexts. This edition is more modular and scalable than earlier versions.

The framework was designed based on ENISA’s needs, but its structure and logic are generic enough to be adopted and adapted by Member States, sectoral authorities and other public or private actors seeking greater transparency, comparability and repeatability in market analysis.

The application of ECSMAF in different configurations will generate empirical feedback on where the framework is most efficient, where changes are needed and where additional guidance, examples or decision rules should be added.

The ENISA team that has developed the framework and is maintaining it will collect lessons learned. Where needed, new versions of ECSMAF will be issued to reflect user feedback, but also legal and policy developments, along with new analytical techniques. ECSMAF will be kept current while preserving the continuity that makes the cybersecurity market analysis performed using the framework comparable and actionable over time.

A Annex: Abbreviations

Abbreviations

CRA	Cyber Resilience Act (Regulation (EU) 2024/2847)
CSA	Cybersecurity Act (Regulation (EU) 2019/881)
ECSMAF	ENISA Cybersecurity Market Analysis Framework
ENISA	European Union Agency for Cybersecurity
EU	European Union
NIS	Network and Information Systems
OSS	open-source software
V	Version

B Annex: Glossary

This glossary [42] defines specific terms used within ECSMAF V3.0 to ensure clarity and consistency in its application.

Methodological concepts, such as qualitative and quantitative research and primary and secondary data, are defined in Annex J (Methodology).

The following terms are included in ECSMAF V3.0:

- **ad hoc request / ad hoc analysis / analysis following an ad hoc request** – unplanned, needs-driven analysis conducted on request, rather than as part of a scheduled cycle;
- **adoption drivers** – factors on the demand/supply sides that increase the uptake of cybersecurity solutions (e.g. regulation, risk, incentives);
- **adoption trends** – observable patterns over time in how cybersecurity solutions/standards/certifications gain traction;
- **advisory group** – an ENISA stakeholder body providing feedback and strategic input;
- **barriers to adoption** – constraints hindering the uptake of cybersecurity solutions (e.g. cost, capability, regulatory complexity);
- **conditional check** – a check to verify whether a certain condition is met;
- **configuration** – the chosen depth, breadth, time/budget/resources and workflow of an analysis (short / long, planned / ad hoc);
- **continuous market monitoring / market monitoring** – a permanent, semi-automated process of tracking the state of a market based on event detection to assess if defined performance rules are maintained;
- **critical infrastructure** – under the NIS 2 Directive refers to entities operating in sectors deemed essential for society's functioning and resilience;
- **data source** – the origin of data;
- **exploratory prompt** – open-ended questions not present in templates, usually used early to explore unbounded areas;
- **formatted data** – data arranged in line with a template/schema to enable analysis and comparability;
- **grey literature** – non-commercial sources (e.g. government reports) used as secondary research inputs;
- **long configuration** – an analysis configuration that requires more than six months;
- **market analysis** – the structured seven-step process for examining a cybersecurity market segment;
- **market segment** – a manageable portion of the cybersecurity market (by technology, service, vertical market segment, etc.);
- **operational readiness** – readiness to implement or respond to an operational need;
- **planned analysis** – a planned, scheduled programmatic analysis (e.g. envisaged in the ENISA programming document);
- **policy context** – the policy/regulatory setting shaping a segment (e.g. the CSA, the NIS 2 Directive);

[42] The definitions provided in this glossary have been drafted to ensure consistency with ENISA's previous publications and to reflect the specific meaning and use of these terms in the context of the current document.

- **power–interest matrix** – a strategic framework used to categorise stakeholders into four quadrants based on two primary factors, namely their power to influence a project and their level of interest in its outcomes [43];
- **recurrent analysis** – an analysis that generates snapshots of market characteristics at discrete time intervals (monthly, annually) for specific product or service segments;
- **short configuration** – an analysis configuration that requires less than six months;
- **stakeholder mapping** – identification and categorisation of relevant actors;
- **standardised data** – consistently defined/structured data, enabling aggregation/comparison;
- **threat landscape** – evolving cyber threats and trends;
- **tractability** – the degree to which something can be effectively addressed given the available tools, resources and institutional conditions;
- **validation** – a cross-cutting activity embedded throughout the process, where analysis choices, findings and outputs are checked against relevant criteria and stakeholder feedback to ensure accuracy and credibility;
- **validation check** – checkpoint for aligning assumptions, refining parameters and verifying outputs throughout the analytical process;
- **value stack** – layers of value created, from basic technical compliance to strategic business outcomes;
- **value stream** – the end-to-end sequence of activities that deliver value to users.

[43] Interreg Central Europe, ‘Enhancing stakeholder engagement through the power–interest matrix’, Interreg Central Europe website, 23 February 2024, https://www.interreg-central.eu/news/enhancing-stakeholder-engagement-through-the-power-interest-matrix/, accessed 11/03/2026.

C Annex: Request Template

REQUESTOR

- **Organisation requesting the market analysis**
  [State the name of the organisation]
- **Contact person in the organisation**
  [State the name and contact details of the person]

PURPOSE OF THE REQUEST

[Describe for which purpose the requestor needs the analysis]

QUESTION(S) THAT THE REQUESTOR WOULD LIKE TO HAVE ANSWERED BY THE ANALYSIS

[Describe what the requestor wants to know – that is, which questions the requestor would like to have answered]

EXPECTED DELIVERY DATE

[Indicate by when the requestor needs the analysis]

SCOPE

[Define the scope of the request, including

- sectors to cover;
- geographical coverage;
- type of products, services or processes to be covered;
- types of incidents to be covered;
- period to be covered (e.g. last six months, last three years, now);
- types of stakeholders to be involved.]

POLICY CONTEXT

- **Relevant legal and policy framework**
  [Summarise EU and national policies or regulations informing the request]

DATA COLLECTION STRATEGY

- **Methodology**
  [Describe the preferred approach to data collection, for example surveys, or interviews with subject matter experts]

- **Target respondents**
  [List the categories of entities from which data will be collected]

- **Data requirements**

  - **Demand side**
    [State what kind of information is needed about those demanding cybersecurity products, services or solutions
    Examples: adoption rates across sectors, budget allocations, procurement trends, skills availability]

  - **Supply side**
    [Describe the kind of information that is needed about those supplying cybersecurity solutions
    Examples: number and types of providers (start-ups, small or medium-sized enterprises, multinationals), product/service categories, market shares, revenues, growth rates, solution maturity, research and development (R & D) intensity]

- **R & D**
  [Say what kind of information is needed about entities generating new knowledge and innovations
  Examples: universities, research centres, technology labs, public/private R & D investments, patents, research outputs, collaborative projects, finance for start-ups and small or medium-sized enterprises, venture capital flows, EU and national funding programmes, private investment trends and funding gaps at different stages (early stage, growth, scale-up)]

- **Regulatory bodies**
  [State the kind of information that is needed about organisations shaping the rules and compliance environment
  Examples: EU/national regulators, supervisory authorities, certification schemes, policy initiatives, standardisation bodies, alignment with EU directives/regulations]

- **Data sources that the requestor can make available to ENISA**
  [List any datasets, surveys, reports or internal records you can share with ENISA to support the analysis
  Examples: proprietary market studies, previous surveys, procurement or incident data, administrative datasets, membership databases, access to expert panels or interviewees]

- **Availability of the requestor to contribute to the analysis (beyond providing data sources)**
  [Describe ways that the requestor could contribute to the analysis other than by providing data sources]

EXPECTED DELIVERABLES AND PREFERRED TIMELINE

HEADING	HEADING
[Insert deliverable]	[Insert date]
[Insert deliverable]	[Insert date]
[Insert deliverable]	[Insert date]
[Insert deliverable]	[Insert date]
[Insert deliverable]	[Insert date]

[Please indicate hard deadlines, if any]

DELIVERABLE FORMAT

[Describe in which kind of format the requestor expects to have the outcome delivered (e.g. raw data in an Excel table, a report in Word/PDF format of around 30 pages)]

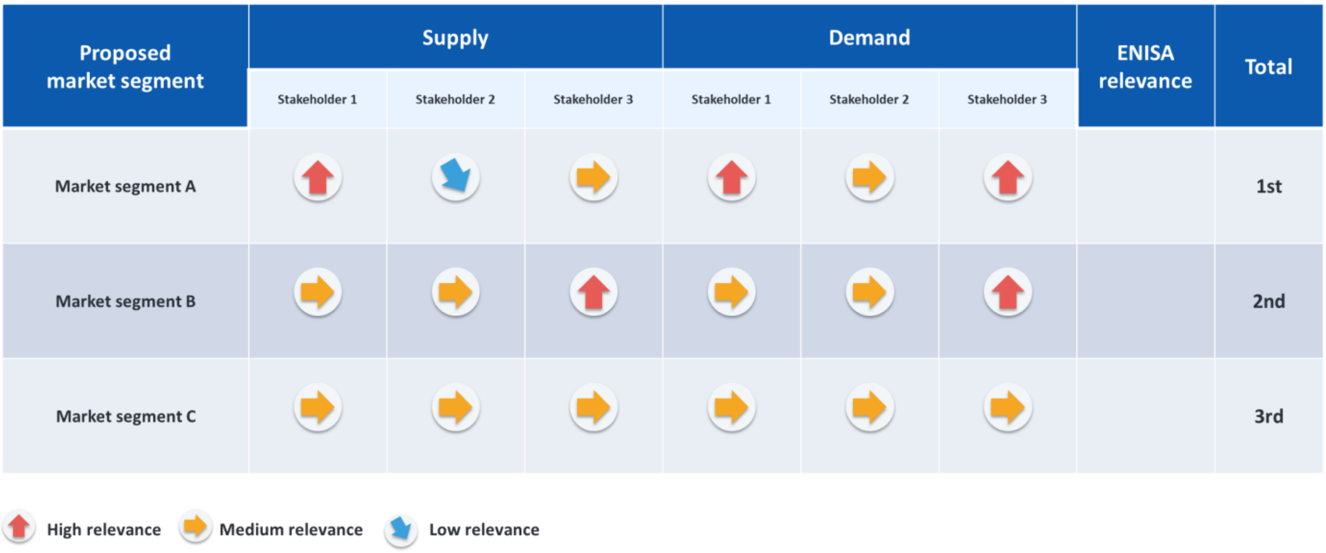
ADDITIONAL NOTES

[Include any relevant considerations, such as data protection, confidentiality and alignment with other initiatives]

D Annex: Template for Assessing the Priority of Market Segments

Table 1 provides an example of how priorities can be established based on preferences expressed by different stakeholders.

Table 1: Template for scoring priority



Proposed market segment	Supply			Demand			ENISA relevance	Total
	Stakeholder 1	Stakeholder 2	Stakeholder 3	Stakeholder 1	Stakeholder 2	Stakeholder 3		
Market segment A	⬆	↘	➡	⬆	➡	⬆		1st
Market segment B	➡	➡	⬆	➡	➡	⬆		2nd
Market segment C	➡	➡	➡	➡	➡	➡		3rd

⬆ High relevance ➡ Medium relevance ↘ Low relevance

E Annex: Criteria for Scoping the Market Analysis

This annex presents a set of criteria for scoping a cybersecurity market analysis. While the original version was applied in the context of a cloud cybersecurity study, the criteria have now been revised and expanded in line with the updated ECSMAF framework. They are designed to be relevant across all cybersecurity market segments and can be tailored depending on the specific configuration of the analysis (e.g. short or long, ad hoc or planned).

The scoping criteria in Table 2 are key to Step 2 (Scope the Market Segment for Analysis) and help shape the survey questions, of which Annex L provides examples.

Table 2: Scoping criteria

SCOPING CATEGORIES	SCOPING CRITERIA
Demand side	• Headquarters and other offices (EU and non-EU, in particular in Africa, Asia, Central Asia, Eastern Europe, Latin America and the Caribbean, the Middle East and North Africa, North America, the Pacific, the Western Balkans, non-EU Western Europe and overseas countries and territories) (*) • Ownership (organisation EU controlled or non-EU controlled). • Profile of demand organisations (sector, size, level of digitalisation). • Geographical coverage (local or international). • Role of the product/service in business continuity and resilience. • Organisational capabilities and maturity required to adopt the product/service. • Contribution to risk mitigation and compliance with regulatory requirements. • Functional needs and gaps between demand requirements and current market offerings. • Demand-side investment strategies and procurement capacity. • Barriers to adoption (financial, technical, organisational, cultural).
Supply side	• Headquarters and other offices (EU and non-EU, in particular in Africa, Asia, Central Asia, Eastern Europe, Latin America and the Caribbean, the Middle East and North Africa (MENA), North America, the Pacific,

	the Western Balkans, non-EU Western Europe and overseas countries and territories) (*) • Ownership (organisation EU controlled, non-EU controlled). • Supplier landscape (size, maturity, financial capacity, market share). • Geographical coverage and delivery models (local or international). • Integration of the product/service in suppliers' value chains and ecosystems. • Capabilities and resources required for large-scale deployment. • Effectiveness of the product/service in addressing threat scenarios. • Gaps in supply relative to emerging demand and regulatory needs. • Supplier innovation and investment strategies (e.g. partnerships, acquisitions). Trends, drivers and systemic barriers in the supply market.
R & D	• R & D investment levels and funding instruments (public, private, public–private partnerships). • Presence of research institutions (universities, labs, consortia, innovation hubs). • Ongoing and emerging research projects relevant to the market segment. • Innovative approaches, disruptive technologies, and patents. • Availability of specialised skills and knowledge transfer mechanisms. • Drivers of and barriers to R & D commercialisation. Alignment of R & D activities with EU cybersecurity priorities and industrial policy.
Regulation and standardisation	• Regulatory scope (sectors, activities and entities covered). • Relevant EU and national regulations (e.g. the NIS 2 Directive, DORA, CRA, the AI Act) shaping demand. • Compliance obligations and their impact on market evolution. • Anticipated changes in regulatory instruments and transition requirements. • Incentives and support mechanisms for regulatory adoption. • Drivers of and barriers to compliance in the market.

	• Standardisation initiatives and stakeholder communities (e.g. ETSI, ISO, CEN/CENELEC). Influence of certification schemes and conformity assessment frameworks.

(*) List of regions taken from https://www.eeas.europa.eu/_en#:~:text=The%20European%20External%20Action%20Service%20%28EEAS%29%20is%20the,and%20the%20interests%20of%20Europeans%20across%20the%20globe (see regions under the ‘EU in the World’ TAB).

NB: CEN, European Committee for Standardization; CENELEC, European Committee for Electrotechnical Standardization; DORA, Digital Operational Resilience Act; ETSI, European Telecommunications Standards Institute; ISO, International Organization for Standardization; OCTs, overseas countries and territories; R & D, research and development.

F Annex: Infrastructure Mapping

Table 3 provides a template to support the identification of the infrastructure underpinning a selected market segment. Infrastructure refers to the technical components, systems, platforms and operational environments that collectively define the architecture of a segment. The aim is to establish a clear map of the infrastructure baseline, to serve as the reference point for subsequent analytical steps.

STEP 1: DEFINE SCOPE

- Name of market segment
- Boundaries of inclusion/exclusion (technologies, services, environments)

STEP 2: IDENTIFY INFRASTRUCTURE COMPONENTS

Table 3: Examples of infrastructure components

CATEGORY	ELEMENTS TO CAPTURE	EXAMPLES (ILLUSTRATIVE)
Core technologies	Fundamental technical building blocks of the segment	Cryptographic algorithms, security protocols
Products and systems	Hardware, software or integrated systems central to the segment	Hardware security modules, security operations centre platforms, cloud servers
Supporting platforms	Digital or technical platforms enabling the functioning of the segment	Middleware, orchestration tools, application programming interfaces
Operational environments	Typical environments where the segment is deployed or operates	Data centres, enterprise information technology networks, operational technology / industrial control systems
Interoperability layers	Standards, certification or compatibility frameworks required for operation	European Telecommunications Standards Institute / International Organization for Standardization standards, European common criteria-based cybersecurity certification scheme
Dependencies	External infrastructures or technologies essential for the functioning of the segment	Semiconductor supply chains, telecommunication networks

STEP 3: CHECK DATA AVAILABILITY

- **Existing sources** (ENISA reports, Eurostat, studies by the European Commission's Joint Research Centre, standards catalogue)
- **Stakeholder inputs** (interviews, workshops, validation sessions)
- **Data gaps** (to be flagged for further collection or provisional mapping)

STEP 4: MAP INFRASTRUCTURE

- Consolidate the elements identified into a visual or tabular infrastructure map.
- Ensure that only infrastructure components are included at this stage (assets, value stacks, threats, requirements, market challenges and stakeholders are addressed later).

G Annex: Examples of Cybersecurity Value Stacks

The structure and content of a typical cybersecurity value stack, broken down into groups, values and elements, is presented in **Table 4**. The information provided builds on work undertaken by ENISA, the European Cyber Security Organisation and the European Commission's Joint Research Centre, updated to reflect current market terminology and technological developments. The structure of value stacks may vary, depending on the sector analysed.

Table 4: Value stack examples

VALUE STACK GROUP	VALUE STACK	VALUE STACK ELEMENTS
R & D and education	Education	• Academia and research institutions dealing with cybersecurity • Professional education and training programmes • Cybersecurity awareness platforms
	R & D	• Cyber threat and vulnerabilities research • Cryptography research • Software and hardware R & D • Standards and certification R & D • Security issues associated with AI and emerging technologies

Software	Application security software	• Application security testing • Vulnerability assessment • Web application firewalls • Secure software development tools
	Cloud security software	• Cloud access security brokers • Cloud security posture management • Cloud workload protection platforms • ‘Software as a service’ security tools
	Data security software	• Encryption software • Prevention of enterprise data loss • Tokenisation software • Database activity monitoring
	Identity and access management software	• Access management • Identity governance and administration • Privileged access management • Multi-factor and user authentication software

		• Zero-trust solutions
	Infrastructure protection software	• End point protection platforms / end point detection and response • Secure email gateways • Secure web gateways • Next-gen antivirus • Extended detection and response platforms
	Operational platforms	• Security information and event management • Threat intelligence platforms • Security orchestration, automation and response • Deception technologies
	Integrated risk management / governance, risk and compliance software	• Digital risk management • Vendor risk management • Business continuity management • Audit and compliance management • Legal and oversight mechanisms of enterprises

Hardware	Network security equipment	• Firewalls / next-generation firewalls • Intrusion detection and prevention systems • Network access control • Network detection and response • Zero-trust network access • Unified threat management
	Hardware security	• Trusted platform modules • Hardware security modules • Secure enclaves
	Biometric security equipment	• Biometric device hardware • Biometric solution software
Distribution	Distribution channels	• Software resale • Hardware resale • Managed services resale
Advisory and consulting	Professional services	• Cybersecurity strategy and risk management advice • Security testing and assessments (penetration testing,

		red/blue teaming) • Design and optimisation of security operations centres • Compliance and audit services • Digital forensics • Project management and staff augmentation
Implementation services	Design and integration	• Security design and architecture • Interoperability and integration services • Technical implementation support
Managed services	Managed response services	• Managed detection and response • Incident response services • Co-managed security operations centre services
	Device and service management	Security device management (maintenance, patching, testing, decommissioning)
	Threat and vulnerability services	• Threat detection and hunting • Vulnerability management

		• Threat intelligence
	Virtualised/'as-a-service' cybersecurity	• Cybersecurity as a service • Security training as a service • User behaviour analytics • Proactive threat hunting
Certification services	Product certification	• Services for product security certification (requirements, evaluation, controls, testing)
	Service and process certification	• Services for certification of processes and operations (audits, gap analysis, accreditation of labs/processes)
	Professional certification	• Certification courses and examinations • Development and maintenance of certification standards • Accreditation of organisations and testing infrastructures

NB: R & D, research and development.

H Annex: Stakeholders

Stakeholder groups include:

- national public authorities, especially cybersecurity authorities;
- EU institutions, bodies and agencies;
- private sector organisations on both the demand and the supply side;
- open-source ecosystem and standardisation bodies;
- international organisations and non-EU countries' national public authorities and cybersecurity authorities;
- research and innovation institutions;
- other ENISA stakeholders.

I Annex: Barriers and Challenges

Table 5 presents barriers and challenges to the fulfilment of requirements for cybersecurity products and services. These elements have been derived from the technical, procedural, business and organisational requirements typically expected of providers. When such requirements are not met, they create obstacles to adoption, weaken trust and limit the effectiveness of cybersecurity solutions. Identifying these barriers at an early stage allows market analyses to highlight structural weaknesses, dependencies and areas where targeted measures or policy interventions may be required.

Table 5: Barriers and challenges to meeting cybersecurity requirements

CATEGORY	BARRIER/CHALLENGE	EXAMPLES/IMPLICATIONS
Technical aspects	Lack of preparedness and prevention capabilities	Service providers unable to anticipate or mitigate incidents effectively
	Insufficient monitoring and detection	Gaps in coverage, delayed detection of threats
	Limited restoration and recovery tools	Slow recovery, prolonged downtime after incidents
	Weak vulnerability and patch management	Exploitable weaknesses persist in protected systems
	Inadequate data protection mechanisms	Exposure of sensitive data, non-compliance with the General Data Protection Regulation
	Lack of multiplatform/multi-device coverage	Inconsistent protection across infrastructure
	Poor scalability for large infrastructures	Providers unable to serve large or complex customers
	Failure to apply standards and good practices	Reduced interoperability, weaker assurance
	Insufficient analytical capacity	Inability to process and correlate large volumes of data
	Lack of capabilities for forensic and artefact analysis	Evidence not preserved in line with international standards, weakening investigations

Processes and procedures	Weak governance, risk and control frameworks	Misaligned cybersecurity strategy
	Absence of formal policies/procedures	Fragmented response, lack of accountability
	Limited emergency coordination	Ineffective crisis management, delayed recovery
	Failure to follow procedural standards	Reduced trust, lack of comparability
	Inadequate support for coordination	Providers unable to manage multiparty or on-site responses
	Insufficient privacy controls	Violation of General Data Protection Regulation, loss of trust
Digital sovereignty	Unclear or insecure data location	Risk of foreign dependency, non-compliance with sovereignty requirements
Business requirements	No proof of concept before contracting	Increased adoption risk, poor solution fit
	Limited support for multivendor environments	Vendor lock-in, reduced interoperability
	Rigid pricing schemes	Exclusion of small or medium-sized enterprises, lack of flexibility in adoption
Service-level agreements and metrics	Lack of customisable service-level agreements	Misalignment with customers' operational needs
	Absence of clear metrics	Inability to measure service quality
Workforce	Shortage of skilled personnel	Limited service capacity, delayed response
	Insufficient expertise/certifications	Lower assurance of service quality
	Inability to handle simultaneous or large-scale incidents	Vulnerability in crisis conditions
	Limited provider training	Workforce not kept up to date on threats and tools
	Limited service capacity	Inability to meet customer demand

Provider organisation	Restricted geographical presence	Lack of on-site response when needed
	Lack of national/EU accreditation	Lower credibility and trust
	Limited language support	Barriers to adoption across Member States

J Annex: Methodology

Choosing an appropriate methodology is a crucial step in any market analysis, as it determines the type of data collected, and how data are gathered and interpreted. ECSMAF recognises a wide spectrum of methods, which can be broadly categorised into qualitative and quantitative approaches, and based on the use of primary and secondary data.

Qualitative versus Quantitative Research

Qualitative research is used to explore people's experiences, perspectives and behaviours. It is interpretative and context driven, relying on open-ended data, for example, from interviews, workshops and document reviews. The goal of this research is to uncover meaning, motivations and patterns, typically analysed through methods such as thematic analysis or discourse analysis.

By contrast, **quantitative research** relies on numerical data to measure and test hypotheses. It seeks to confirm assumptions, identify trends and establish cause–effect relationships, drawing on structured surveys, statistical indicators or modelling exercises ([44]).

Both approaches can be combined to enrich an ECSMAF analysis, with qualitative methods providing depth and quantitative methods providing breadth and comparability.

Primary versus Secondary Data

The term '**primary data**' refers to information collected directly from its original source by an analyst, for example through statistical surveys, interviews or specially designed instruments intended for the study at hand.

The term '**secondary data**' refers to information that is redistributed by an organisation or individual other than the one that collected the original data. These secondary sources may disseminate the data as is or transform them through processes such as further aggregation, reclassification or seasonal adjustment. In ECSMAF, secondary data may include administrative records, existing datasets, regulatory filings or other processed data originating from primary statistical sources ([45]).

Guide to Research Methods

Some guidance on research methods is provided below[46]:

Quantitative Research Designs (Experimental and Quasi-experimental)

- **Experimental Research**

Experimental designs establish causality by randomly assigning subjects to groups and manipulating independent variables while controlling conditions. They are the most rigorous way to test

[44] Elsevier Author Services, 'Choosing the Right Research Methodology: A Guide for Researchers Elsevier Author Services website, https://scientific-publishing.webshop.elsevier.com/research-process/choosing-the-right-research-methodology-a-guide-for-researchers/ (accessed 11/03/2026).

[45] Eurostat, '*Glossary: Secondary source of statistical data'*, Eurostat website, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Secondary_source_of_statistical_data (accessed 11/03/2026).

[46] Adapted from Edmonds, W. A. and Kennedy, T. D., *An Applied Guide to Research Designs: Quantitative, qualitative, and mixed methods*, 2nd edition, SAGE Publications, 2017.

interventions. In ECSMAF, experimental reasoning can underpin controlled pilots of cybersecurity tools or policy interventions.

- **Quasi-experimental Research**

Quasi-experiments mirror experimental designs but lack full randomisation. They are widely used in applied research where random assignment is impractical. In the context of ECSMAF, these designs may be applied when assessing regulatory pilots or evaluating market incentives without strict control over conditions.

- **Between-Subjects Approaches**

These designs compare groups exposed to different conditions. Pretest–post-test or post-test-only structures measure changes attributable to interventions. With regard to ECSMAF, between-subjects approaches could be used to compare organisations adopting a new cybersecurity practice with those not doing so.

- **Regression-Discontinuity Approach**

This approach assigns groups based on a cut-off score on a pre-intervention variable, allowing the estimation of causal effects. In the context of ECSMAF, it may be used to evaluate funding eligibility criteria, for example for grants for small or medium-sized enterprises based on size thresholds.

- **Within-Subjects Approaches**

Within-subjects designs expose the same subjects to multiple conditions, allowing direct comparison. Variants include repeated-measures, switching-replications, crossover and Latin-square designs. With regard to ECSMAF, such designs could assess the same set of organisations under varying policy or technological conditions.

- **Factorial Designs**

Factorial designs test combinations of two or more factors to examine both individual and interactive effects. In the context of ECSMAF, they could be applied to study the interaction between regulatory pressure and financial incentives in shaping cybersecurity adoption.

- **Solomon *N*-group Designs**

These complex designs combine multiple groups with varying pretest and intervention exposures to isolate testing effects. Though rarely used, they can enhance robustness in ECSMAF pilot studies where multiple confounding factors must be considered.

- **Single-Case Approaches**

Single-case designs intensively examine one unit under varying conditions (A–B, A–B–A, A–B–A–B[47], multiple baselines, changing criterion, small *n*[48]). In the context of ECSMAF, they could be used in analyses involving niche technologies, specialised suppliers or unique regulatory contexts where large samples are unavailable.

[47] ‘A’ stands for ‘Baseline’ and ‘B’ for ‘Intervention’.

[48] Small *n* designs are focused on one individual or on a very limited number of participants.

Quantitative Research Designs (Non-experimental)

- **Benchmarking**

Benchmarking compares the performance, processes or practices of a given sector, country or organisation against reference models or peers. It is often quantitative but may also involve qualitative comparison. With regard to ECSMAF, benchmarking can be applied to compare cybersecurity markets and frameworks against international baselines, to identify strengths and gaps.

- ***Ex Post Facto* and Post-test-only Designs**

These designs analyse outcomes after the fact, without manipulating variables. They may be applied in the context of ECSMAF when examining the impact of a cyber incident or of implementing a regulation.

- **Observational Approaches**

Observational research tracks naturally occurring behaviours or conditions without manipulation. Variants include explanatory designs, predictive designs, regression analyses, correlational studies and causal modelling. With regard to ECSMAF, these approaches can be used when identifying associations, for example, between research and development (R & D) investment and supplier maturity.

- **Survey Approaches**

Surveys are widely used non-experimental designs, administered cross-sectionally or longitudinally. They provide structured, quantitative data across large samples. In the implementation of ECSMAF, surveys can be employed to capture demand- and supply-side perspectives, measure adoption rates and map barriers to deployment.

- **Trend Analysis**

Trend analyses examine data over time to detect patterns, shifts and trajectories. They rely primarily on quantitative indicators such as adoption rates, R & D spending or incident frequencies, but may be complemented by qualitative interpretation. Through ECSMAF, trend analyses are applied to monitor changes in cybersecurity demand and supply and to anticipate emerging pressures on the market.

Qualitative Research Designs

- **Case Study**

Case studies examine bounded cases (of organisations, technologies or sectors) in their real-life contexts. Variants include single or multiple and holistic or embedded designs. In the context of ECSMAF, case studies can be used to illustrate adoption patterns, regulatory implementation or innovation dynamics.

- **Grounded Theory**

Grounded theory inductively builds theory from systematically coded data. Variants include systematic, emerging and constructivist approaches. With regard to ECSMAF, grounded theory may reveal how stakeholders interpret cybersecurity risks and regulatory obligations.

- **Ethnography**

Ethnographic research immerses the researcher in a cultural or organisational setting over time. Variants include realist, critical or case-based ethnography. In applying ECSMAF, this kind of research may be conducted to understand practices within cybersecurity communities or supply-chain networks.

- **Narrative Research**

Narrative enquiry focuses on personal stories and accounts as a means of understanding experiences. Variants include descriptive, explanatory and critical narratives. As regards ECSMAF, narrative methods could highlight how small or medium-sized enterprises describe their cybersecurity journeys.

- **Phenomenology**

Phenomenological research explores lived experience to identify the essence of a phenomenon. Approaches include existential, transcendental, hermeneutic and case-based phenomenology. In the context of ECSMAF, this design could be used to capture the experience of end users affected by cyber incidents or measures implemented to achieve regulatory compliance.

- **Stakeholder Mapping**

Stakeholder mapping involves the systematic identification and categorisation of stakeholders according to their roles, influences and interests. Tools such as power–interest matrices help prioritise engagement and highlight potential tensions. In the implementation of ECSMAF, stakeholder mapping guides data collection strategies and ensures the balanced representation of perspectives in market analyses.

- **Workshops and Expert Validation**

Workshops bring together stakeholders in facilitated sessions to discuss, test and refine findings. As a qualitative method, they allow interaction, the negotiation of meaning and joint validation. In applying ECSMAF, workshops are crucial for aligning perspectives across demand, supply, R & D and regulatory stakeholders, ensuring that analyses reflect collective expertise.

Mixed Methods Designs

- **Convergent-Parallel Approach**

This design collects qualitative and quantitative data simultaneously and integrates them for interpretation. Variants include parallel databases, data transformation, data validation and multilevel designs. In the context of ECSMAF, such approaches ensure that survey statistics and stakeholder interviews reinforce each other.

- **Delphi Method**

The Delphi method is a structured expert elicitation process, typically conducted over multiple rounds. Experts anonymously provide judgements, review aggregated feedback and refine their responses until consensus or stability is reached. As part of ECSMAF, Delphi-style methods can be used to validate assumptions, estimate uncertain parameters and test future-oriented hypotheses.

- **Embedded Approach**

Embedded designs place one method within another, such as a qualitative component in a larger survey or experiment. Variants include experiment-embedded, correlational-embedded and case-study-embedded designs. As regards ECSMAF, these may be used to enrich quantitative findings with explanatory detail.

- **Explanatory-Sequential Approach**

This design involves collecting quantitative data first, then follows up qualitatively to explain results. Variants include follow-up explanations and participant selection models. The approach can be adopted as part of ECSMAF to interpret unexpected survey outcomes through targeted interviews.

- **Exploratory-Sequential Approach**

This design begins with qualitative exploration, then builds in quantitative measures to test findings. Variants include instrument, theory and treatment development. The approach could be applied in the application of ECSMAF to build survey instruments from stakeholder interviews.

- **Mixed-Methods-Case and Single-Case Approaches**

These designs combine case study logic with mixed methods or apply mixed methods to single-case studies (e.g. sequential A–B–A designs). They may be used in the context of ECSMAF to study a single sector, by combining in-depth interviews with adoption statistics.

- **Network Analysis**

Network analyses study the structure and dynamics of relationships between actors. Using graph-based models, they reveal central actors, clusters and flows of information or resources. With regard to ECSMAF, network analyses can highlight dependencies and vulnerabilities in cybersecurity ecosystems, mapping how suppliers, regulators and demand-side organisations are interconnected.

- **Scenario Analysis / Strategic Foresight**

Scenario analyses explore plausible futures by combining qualitative narratives with quantitative projections. Strategic foresight methodologies place ECSMAF findings in long-term contexts, examining how regulatory, technological and market drivers could shape different trajectories. These methods are especially relevant in planned analyses to anticipate risks and opportunities for EU cybersecurity markets.

Action Research

Action research integrates enquiry with direct intervention in a cyclical process of planning, acting, observing and reflecting. It is participatory and collaborative, involving stakeholders as co-producers of knowledge. In the context of ECSMAF, action research approaches are well suited to regulatory sandboxes, innovation pilots or capacity-building initiatives where iteration and learning are essential.

K Annex: Data Collection

Table 6 and Table 7 provide an overview of the main tools and sources used for data collection in ECSMAF market analyses. The tools should be selected based on the type of data required (primary or secondary), the scope of the market segment and the configuration of the analysis (short or long, ad hoc or planned).

Table 6: Data collection tools and sources

EXAMPLES OF TOOLS/SOURCES	CATEGORY	DESCRIPTION AND APPLICATION TO ECSMAF
Primary research		
EU survey and other (online) survey tools	Online survey platforms	Tools for designing and distributing structured questionnaires. For primary data collection from demand, supply, research and development, and regulatory stakeholders.
Tools for virtual meetings	Interview and workshop platforms	Tools for remote interviews, focus groups and workshops (with recording options). For expert consultations, validation rounds and stakeholder engagement.
Tools for data capture	Data management	Tools widely used to collect, clean and structure quantitative data. For initial storage, filtering and harmonisation of data before deeper analysis.
Secondary research		
National, European and international institutions' official statistical databases (e.g. the Eurostat database, the OECD Data Explorer,	Institutional	Official websites of national, EU or international institutions providing statistical data and reports. For benchmarking and to determine contextual indicators, to

the World Bank's DataBank) and reports		complement data and enable broader comparisons.
Official regulatory and legal databases (e.g. EUR-Lex)	Institutional	Provide access to legislation, regulatory instruments, policy instruments, legal initiatives, etc. To retrieve information on relevant legal, regulatory and policy frameworks.
Standardisation bodies' databases	Standardisation	Offer global policy perspectives, standardisation roadmaps and related regulatory context that shape adoption readiness and compliance fit. To retrieve information on standards and compliance.
Databases providing information about businesses, investments, acquisitions, ownership, etc.	Business and finance	Provide financial information; corporate data; and data on market shares, supply-side profiling, investment, etc. To establish demand and supply demographics.
Websites and databases of technology companies and integrators	Technology companies	Publish security landscape reports, technical white papers and deployment roadmaps grounded in direct operational data and global client experience.
Consumer associations	Consumer	
Universities and research centres	Academia / research and innovation	Deliver rigorous academic studies, technical assessments and early-stage foresight analyses of emerging or disruptive technologies.
Industry associations and technical alliances	Industry	Issue white papers, best practice guides and frameworks that track developments in specific sectors or technologies, often bridging industry and regulation.
Market analysts and consultancies	Consultancy	Provide insights on technology-related market trends, adoption

		forecasts, competitive dynamics and vendor landscapes. To identify which technologies are commercially viable and gaining traction.
Investment banks and venture funds	Business and finance	Offer data on funding flows, start-up ecosystems and investment theses that indicate where capital is driving technological growth and innovation hotspots.
Think tanks and policy institutes	Research and innovation	Provide strategic scenarios, geopolitical assessments and long-range policy analyses that enrich the foresight and risk contexts.
Technology news outlets and trade publications	Media	Highlight the most recent developments, emerging applications, and shifts in market sentiment that may not yet appear in formal studies, offering early signals of change.
Open-source repositories (e.g. GitHub)	Collaborative platform	Platforms containing collaborative software projects. To observe innovation in open-source cybersecurity tools.
Research databases (e.g. CORDIS)	Research and innovation	Provide information on collaborative software projects and could be used to retrieve information on innovation in open-source cybersecurity tools. To identify research developments, drivers, challenges, etc.

NB: CORDIS, Community Research and Development Information Service; OECD, Organisation for Economic Co-operation and Development.

Data Collection Tips

- **Define data needs early.** Clarify whether the analysis requires primary or secondary data, and which stakeholder categories (demand, supply, research and development, regulation) are essential. This avoids redundant data collection and ensures efficiency.
- **Balance breadth and depth.** Short analyses should prioritise speed and reliability, relying more on secondary sources. Long analyses can involve broader surveys, interviews and foresight exercises.

- **Ensure consistency across tools.** Use predefined metrics (e.g. Excel sheets for quantitative indicators, coding schemas for interviews) to maintain comparability across different analysts and time frames.
- **Validate inputs at multiple stages.** Where possible, cross-check survey data with interviews, or benchmark company datasets against Eurostat / Organisation for Economic Co-operation and Development figures. Triangulation enhances reliability.
- **Document sources meticulously.** Record not just data, but also metadata: when the data were collected, from whom, and under what conditions. This supports transparency and reproducibility.
- **Respect confidentiality and ensure compliance with the General Data Protection Regulation / Data Protection Regulation for EU institutions, bodies, offices and agencies compliance.** Sensitive information from companies or individuals must be handled in line with EU data protection requirements, especially when obtained from interviews and survey responses.
- **Leverage stakeholder engagement.** Use workshops and expert validation sessions not only for analysis but also as an opportunity to refine data collection instruments and fill gaps.
- **Data comparison.** Use standardised indicators, reference years and harmonised taxonomies to facilitate comparability.

Data Sources

Table 7: Example of how to document data sources

TYPE OF SOURCE	WHY IT WAS NEEDED

L Annex: Examples of Survey Questions for Each Stakeholder Type

The following questionnaire template is designed to guide the structured collection of information from stakeholders that is relevant to cybersecurity market analysis. It provides a consistent set of question topics that can be adapted to different stakeholder groups (demand-side organisations, supply-side actors, research and development entities, and regulatory bodies).

The questions should capture essential details about organisations and their activities, standards and certification practices, regulatory contexts, incident experiences, and perspectives on market evolution and innovation. While the structure should remain the same for all stakeholders, the wording of individual questions can be tailored to reflect the specific role of each group within the market segment. Moreover, questions may be adapted based on the specific focus of the analysis.

Demand-Side Question Template

General Information

- Consent to privacy policy and data handling (**mandatory**).
- Organisation name.
- Legal structure of the organisation.
- Country of establishment/headquarters.
- Headquarters (EU and non-EU, in particular in Africa, Asia, Central Asia, Eastern Europe, Latin America and the Caribbean, the Middle East and North Africa, North America, the Pacific, the Western Balkans, non-EU Western Europe (particularly Andorra, Iceland, Liechtenstein, Monaco, Norway, San Marino, Switzerland and the United Kingdom) and overseas countries and territories (49).
- Other offices (EU and non-EU, in particular in Africa, Asia, Central Asia, Eastern Europe, Latin America and the Caribbean, the Middle East and North Africa, North America, the Pacific, the Western Balkans, non-EU Western Europe (particularly Andorra, Iceland, Liechtenstein, Monaco, Norway, San Marino, Switzerland and the United Kingdom) and overseas countries and territories (50).
- Control status (established in EU / European Economic Area / European Free Trade Association, ownership).

(49) List of regions taken from https://www.eeas.europa.eu/_en#:~:text=The%20European%20External%20Action%20Service%20%28EEAS%29%20is%20the,and%20the%20interests%20of%20Europeans%20across%20the%20globe(accessed 21/11/2025).

(50) List of regions taken from https://www.eeas.europa.eu/_en#:~:text=The%20European%20External%20Action%20Service%20%28EEAS%29%20is%20the,and%20the%20interests%20of%20Europeans%20across%20the%20globe (accessed 21/11/2025).

- Enterprise size (micro, small, medium, large) [51].
- Annual turnover / operational budget.

Organisation Profile

- Private or public entity.
- Number of employees (total).
- Sector of activity.
- Budget dedicated to cybersecurity, or the specific cybersecurity product(s) or service(s) [52] (percentage of turnover).
- Internal cybersecurity management capabilities (yes/no).
- If yes, areas covered in-house.

Use of Cybersecurity Services

- Cybersecurity products or services currently implemented.
- Service delivery options used (on-premises, cloud based, hybrid, outsourced).
- Services planned for future procurement (list by category).
- Criteria for selecting service providers.
- Frequency of re-evaluating selection criteria.

Standards and Certifications

- Standards relevant to the specific product(s) or service(s) (international, EU, national).
- Certifications required from providers (product, service, professional staff, tools).
- Most important certifications demanded.
- Gaps in current standards or certifications.
- Expectations for levels of assurance.
- Cases where self-assessment would be acceptable.
- Perceived advantages of and barriers to certification.

Regulation and Compliance

- Applicable legislation (international, cross-sector EU, sector-specific EU, national).
- Classification of the organisation based on the NIS 2 Directive (essential, important, other).

[51] For definitions of micro, small, medium and large enterprises, see Eurostat, ‘Information on data’, Eurostat website, accessed 21 November 2025, https://ec.europa.eu/eurostat/web/structural-business-statistics/information-data#Enterprise%20size%20classes%20(including%20SMEs)(accessed 21/11/ 2025).

[52] The phrase ‘specific cybersecurity product(s) or service(s)’ in this annex means the cybersecurity product(s) or service(s) the analysis focuses on.

Incidents and Risks

- Awareness of significant incidents in services used or supply chain.
- Impact of incidents (technical, operational, reputational).
- Whether incidents triggered mandatory reporting.
- Time to resolution of major incidents.

Market Evolution

- Main technological challenges to delivering the specific cybersecurity product(s) or service(s).
- Barriers to adoption and/or upgrading of cybersecurity services.
- Key political, economic, societal, legal or environmental trends affecting the market.
- Gaps observed between demand and supply
- Main technological drivers of cybersecurity service adoption.
- Main business drivers of cybersecurity service adoption.

Innovation and Research

- Start-ups.
- Scale-ups.
- EU-based companies with high innovation potential in relevant areas.
- Priority research topics for the specific cybersecurity product(s) or service(s).

Final Input

- Free space for additional remarks.

Supply-Side Question Template

General Information

- Consent to privacy policy and data handling (**mandatory**).
- Company name.
- Legal structure of the organisation.
- Headquarters (EU and non-EU, in particular in Africa, Asia, Central Asia, Eastern Europe, Latin America and the Caribbean, the Middle East and North Africa, North America, the Pacific, the Western Balkans, non-EU Western Europe (particularly Andorra, Iceland, Liechtenstein, Monaco, Norway, San Marino, Switzerland and the United Kingdom) and overseas countries and territories ([53]).

[53] List of regions taken from https://www.eeas.europa.eu/_en#:~:text=The%20European%20External%20Action%20Service%20%28EEAS%29%20is%20the,and%20the%20interests%20of%20Europeans%20across%20the%20globe (accessed 21/11/2025).

- Other offices (EU and non-EU, in particular in Africa, Asia, Central Asia, Eastern Europe, Latin America and the Caribbean, the Middle East and North Africa, North America, the Pacific, the Western Balkans, non-EU Western Europe (particularly Andorra, Iceland, Liechtenstein, Monaco, Norway, San Marino, Switzerland and the United Kingdom) and overseas countries and territories ([54]).
- Establishment and control status (established inside or outside EU, EU controlled or not EU controlled).
- Enterprise size (micro, small, medium, large) ([55]).

Company Profile

- Number of employees (total).
- Annual turnover / operational budget.
- Percentage of turnover generated by cybersecurity-related activities.
- Number of employees dedicated to the specific cybersecurity segment under analysis.
- Use of external associates or contractors (percentage of workforce).

Customer Base

- Main customer sectors served (multiple choice and open field).
- Main geographical markets where the company generates turnover.

Products and Services

- Portfolio of cybersecurity products or services offered.
- Delivery models (on-premises, cloud based, hybrid).
- Value proposition (multiple choice and open field).

Standards and Certifications

- Relevant standards applied (international, EU, national, private).
- Certifications held (product, service, professional staff).
- Frequency of certification renewal.
- Perceived gaps in standards or certifications.
- Main certifications demanded by customers.
- Motivation for and benefits of certification (compliance, trust, competitive advantage, etc.).

[54] List of regions taken from https://www.eeas.europa.eu/_en#:~:text=The%20European%20External%20Action%20Service%20%28EEAS%29%20is%20the,and%20the%20interests%20of%20Europeans%20across%20the%20globe (accessed 21/11/2025).

[55] For definitions of micro, small, medium and large enterprises, see Eurostat, 'Information on data', Eurostat website https://ec.europa.eu/eurostat/web/structural-business-statistics/information-data#Enterprise%20size%20classes%20(including%20SMEs) (accessed 21/11/2025).

- Barriers or challenges to certification.

Requirements and Regulation

- Customer requirements most frequently encountered.
- Relevant regulations (international, EU, sector specific, national).

Incidents and Risks

- Awareness of significant incidents in service provisioning or supply chain.
- Impact of incidents (technical, operational, legal, reputational).
- Whether incidents triggered mandatory reporting.
- Average time to resolution of incidents.

Market Evolution

- Key technological challenges to service delivery.
- Barriers to adoption and/or upgrading of the specific cybersecurity product(s) or service(s).
- Political, economic, societal, legal or environmental trends affecting the market.
- Main technological drivers of cybersecurity service adoption.
- Main business drivers of cybersecurity service adoption.

Innovation Potential

- Start-ups.
- Scale-ups.
- EU-based companies with high innovation potential in emerging areas (AI, internet of things, convergence of operational technology with information technology, threat detection, automation, metrics / service-level agreements, digital supply chains, remote work, legal/economic issues).

Final Input

- Free space for additional remarks.

Regulatory Bodies Question Template

General Information

- Consent to privacy policy and data handling (**mandatory**).
- Organisation name.
- Legal structure of the organisation.
- Country of establishment/headquarters.

- Geographical presence (offices, representation).
- Number of employees (total).
- Annual turnover / operational budget.
- Percentage of budget dedicated to cybersecurity, or specific product(s) or service(s)

Standards and Certifications

- Most important standards relevant to regulatory practices in cybersecurity / market segment.
- Most-demanded certifications (top three).
- National certification schemes in place for the specific cybersecurity product(s)/service(s) (yes/no, specify).
- Gaps in standards necessary to support certification (up to three, by standard and gap).
- Whether certifications should address different service levels or levels of assurance.
- Awareness of accreditation programmes to certify cybersecurity services (yes/no, specify).
- Experience in certifying services (organisations or staff, national or international).
- Key challenges to developing competence to assess/certify services.
- Estimated time required to gain competence (years).

Regulation and Policy Context

- International regulations relevant to the organisation's remit.
- Cross-sector EU regulations.
- Sector-specific EU regulations.
- National regulations.

Perceptions of Certification

- Key advantages of and incentives for certification.
- Barriers and constraints to, or inhibitors of, certification.

Market Oversight and Incidents

- Most relevant threats that the specific cybersecurity product(s) or service(s) can reduce.
- Requirements that the specific cybersecurity product(s) or service(s) are best positioned to address.
- Awareness of significant incidents in the country related to the specific cybersecurity product(s) or service(s) (yes/no).
- Impact of incidents.
- Whether incidents were subject to mandatory reporting (to a regulatory body, the government or data subjects).

Innovation and Change

- Accreditation programmes or initiatives known to the organisation.
- Emerging gaps in regulatory frameworks.
- Observed trends in or challenges to supervising the delivery of the specific cybersecurity product(s) or service(s).

Final Input

- Free space for additional remarks.

Research and development Question Template

General Information

- Consent to privacy policy and data handling (**mandatory**).
- Organisation name.
- Legal structure of the organisation.
- Country of establishment/headquarters.
- Geographical presence (offices, subsidiaries, research centres).
- EU establishment and ownership status.

Organisation Profile

- Approximate annual budget for research projects (million EUR).
- Percentage of research budget dedicated to cybersecurity, or the specific cybersecurity product(s) or service(s).
- Number of research staff.
- Number of staff dedicated to cybersecurity research.
- Scientific outputs (e.g. research papers, publications).
- Innovation outputs (e.g. patents registered yearly).
- Targeted technology readiness levels in cybersecurity research.

Research Focus

- Information technology developments expected to affect research (positive or negative) related to the specific cybersecurity product(s) or service(s).
- Cybersecurity threats most necessary to address in ongoing or planned research.
- Requirements considered in research projects (e.g. technical, procedural, regulatory, user).
- Discovery of vulnerabilities in products and infrastructures (including open source) related to the specific cybersecurity product(s) or service(s).

Funding

- Main sources of research budgets/grants.
- Ease of access to cybersecurity research funding.
- Key difficulties in accessing or securing funding.
- Initiatives or actions seen as most likely to benefit from research funding.

Drivers and External Factors

- Political, economic, societal, legal or environmental drivers of research/innovation.
- External factors affecting the research landscape (e.g. nation-sponsored attacks, fraud, interception).
- Internal market effects (e.g. regulation, deployment, network effects, bottlenecks).

Innovation Potential

- Research projects or companies with high innovation potential in cybersecurity services.
- Gaps or niches identified in the cybersecurity services market (up to three).
- Start-ups.
- Scale-ups.

Final Input

- Free space for additional remarks.

M Annex: Coding Schemas

Coding schemas are structured frameworks used to systematically classify and interpret qualitative data (for an example, see Table 8). They ensure consistency across coders, facilitate the comparison of results and allow qualitative findings to be integrated with quantitative indicators where necessary.

Template Structure

Code

A short, descriptive label assigned to a segment of text (e.g. ‘regulatory barriers’, ‘adoption drivers’).

Definition

A clear explanation of what the code means, including boundaries (what counts and what does not).

Category/Dimension

The higher-level theme the code belongs to (e.g. demand-side, supply-side, regulation, research and development (R & D)).

Example Extract

A verbatim quotation or data excerpt illustrating the code’s application.

Notes

Reflections on how the code was applied or links to other codes, or emerging insights.

Table 8: Example of a coding schema

CODE	DEFINITION	CATEGORY/ DIMENSION	EXAMPLE EXTRACT	SOURCE	Notes
Adoption drivers	Factors encouraging or accelerating the uptake of cybersecurity tools or services	Demand-side	‘We adopted X to comply with NIS 2’ (small or medium-sized enterprise).	Source X	Strong link to ‘regulatory incentives’
R & D funding gaps	Mentions of insufficient financial support for research or innovation	R & D	‘No EU programme covers early-stage testing.’	Source Y	May be connected to ‘market fragmentation ’

Supplier capabilities	Descriptions of the technical or organisational capacities of providers	Supply-side	‘Our company lacks skilled staff for AI security.’	Source Z	Cross-check with survey data from Q7

NB: Q, question.

N Annex: Example Table of Contents for Market Analysis Report

The structure of the following table of contents reflects the main elements of an ENISA market analysis. The inclusion and depth of individual sections may vary depending on the configuration of the analysis (short or long, ad hoc or planned).

Proposed Table of Contents

Executive Summary

1. Introduction

1.1 Aim of the Report
1.2 Legal and Policy Context
1.3 Scoping of the Market Segment
1.4 Data Collection Methods
1.5 Target Audience of the Report
1.6 Structure of the Report

2. Stakeholder Landscape

2.1 Demographics of Demand, Supply, Regulators, Research and Development
2.2 Financial and Capability Profiles

3. Market Structure and Dynamics

3.1 Scope of Products/Services and Their Usage Patterns
3.2 Adoption Trends and Deployment Horizon

4. Functional and Security Requirements

4.1 Threat Exposure and Cybersecurity Requirements
4.2 Incident Management, Vulnerabilities and Risk Patterns

5. Market Drivers and Barriers

5.1 Regulatory and Compliance Drivers
5.2 Technological and Innovation Drivers (including Research and Development Insights)
5.3 Barriers to Adoption and Market Challenges

6. Market Trends and Future Outlook

6.1 Market Size, Evolution and Forecasts
6.2 Emerging Themes of Research and Innovation
6.3 Strategic Opportunities and Foresight Indicators (if applicable)

7. Concluding Remarks

7.1 Key Findings and Strategic Trends
7.2 Major Market Gaps
7.3 Regulatory Insights and Foresight Elements

Annexes

Annex A – Abbreviations
Annex B – Scoping Criteria
Annex C – Data Collection and Methodological Tools
Annex D – Data Analysis Tools and Coding Templates
Annex E – Glossary
Annex F – References

O Annex: Examples of Report Infographics

This annex provides examples of visualisation types to refer to in the visualisation of market analyses. They can be adapted to different configurations and tailored to the analytical objectives. The purpose is to ensure consistency across outputs while allowing flexibility in presenting data clearly to stakeholders.

Market Composition and Size

- Pie charts show the distribution of market shares by provider type, product category or geography.
- Stacked bar charts show the segmentation of revenues across supply-side actors or demand sectors.

Stakeholder Mapping

- Power–interest matrices show the positioning of stakeholders according to influence and interest.
- Network diagrams enable the visualisation of relationships between stakeholders, supply chains or ecosystems.

Legislation, Standards and Certification

- Tables with icons / colour coding can be used to map standards and certification schemes by applicability.
- Heat maps show adoption levels or compliance gaps across regions/sectors.

Threats and Incidents

- Timeline infographics show the evolution of incidents or emergence of threat vectors over time.
- Risk matrices indicate the likelihood versus the impact of scenarios.

Data Analysis and Trends

- Line graphs show trends in investments, research and development outputs or incidents over time.
- Bar charts provide comparative statistics for Member States or sectors.
- Radar charts enable capability or readiness benchmarking (e.g. based on the adoption of specific technologies).

Workflows and Processes

- Flow charts outline the steps of ECSMAF workflows or validation loops.

- Gantt charts provide timelines of market analysis activities.
- Infographic roadmaps enable comparison between short- and long-configuration workflows.

P Annex: Practical Checklists for Analysts

This annex provides operational checklists aligned with the seven ECSMAF steps. Each checklist is indicative and should be adapted to the specific configuration (short or long, ad hoc or planned).

Step 1: Initiate the Analysis

☐ Confirm mandate, objectives and resources (time, budget, expertise)

☐ Capture requestor's requirements (if ad hoc)

☐ Ensure alignment with ENISA's strategic priorities and regulatory context

☐ Define validation criteria and follow-up mechanism

Step 2: Scope the Market Segment for analysis

☐ Define boundaries: sector, geography, time frame and stakeholders

☐ Assess the feasibility of data collection with the resources available

☐ Select and adapt scoping criteria

☐ Validate scope internally and/or with stakeholders

Step 3: Analyse the Market Segment

☐ Map infrastructure

☐ Identify assets, value stack elements, and threats

☐ Define security requirements and market challenges

☐ Map relevant stakeholders

☐ Validate segment characterisation

Step 4: Describe the ‘What’ and the ‘How’

☐ Formulate guiding questions

☐ Identify primary and secondary data sources

☐ Select data collection methods and prepare tools

☐ Ensure data triangulation

☐ Identify bias mitigation measures

☐ Identify measures for assuring data quality

☐ Validate the design of the data collection and engagement strategy

Step 5: Collect the Data

☐ Engage stakeholders using appropriate methods

☐ Document provenance, metadata and confidentiality safeguards

☐ Ensure compliance with the General Data Protection Regulation and ethical standards

☐ Ensure data quality

☐ Ensure the absence of bias

☐ Validate the completeness and consistency of data

Step 6: Analyse the Data

☐ Prepare analysis tools

☐ Clean, harmonise and structure the dataset

☐ Extract key findings and compare views across sources

☐ Validate the robustness and credibility of results

Step 7: Present and Disseminate the Results

☐ Draft report

☐ Create visuals where appropriate

☐ Define dissemination channels and target audiences

☐ Assess the effectiveness of dissemination and compile lessons learned

Q Annex: Template for Documenting Lessons Learned

Successes

Number	Success	Reference step(s) / cross-cutting activity (or activities)	Factor(s) contributing to the success	Recommendations(s) for replicating it in the future
1				
2				
3				
[…]				

Challenges/Failures

Number	Challenge/failure	Reference step(s) / cross-cutting activity (or activities)	Root cause	Recommendation(s) for avoiding it / better mitigating it in the future
1				
2				
3				
[…]				

TP-01-25-035-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union