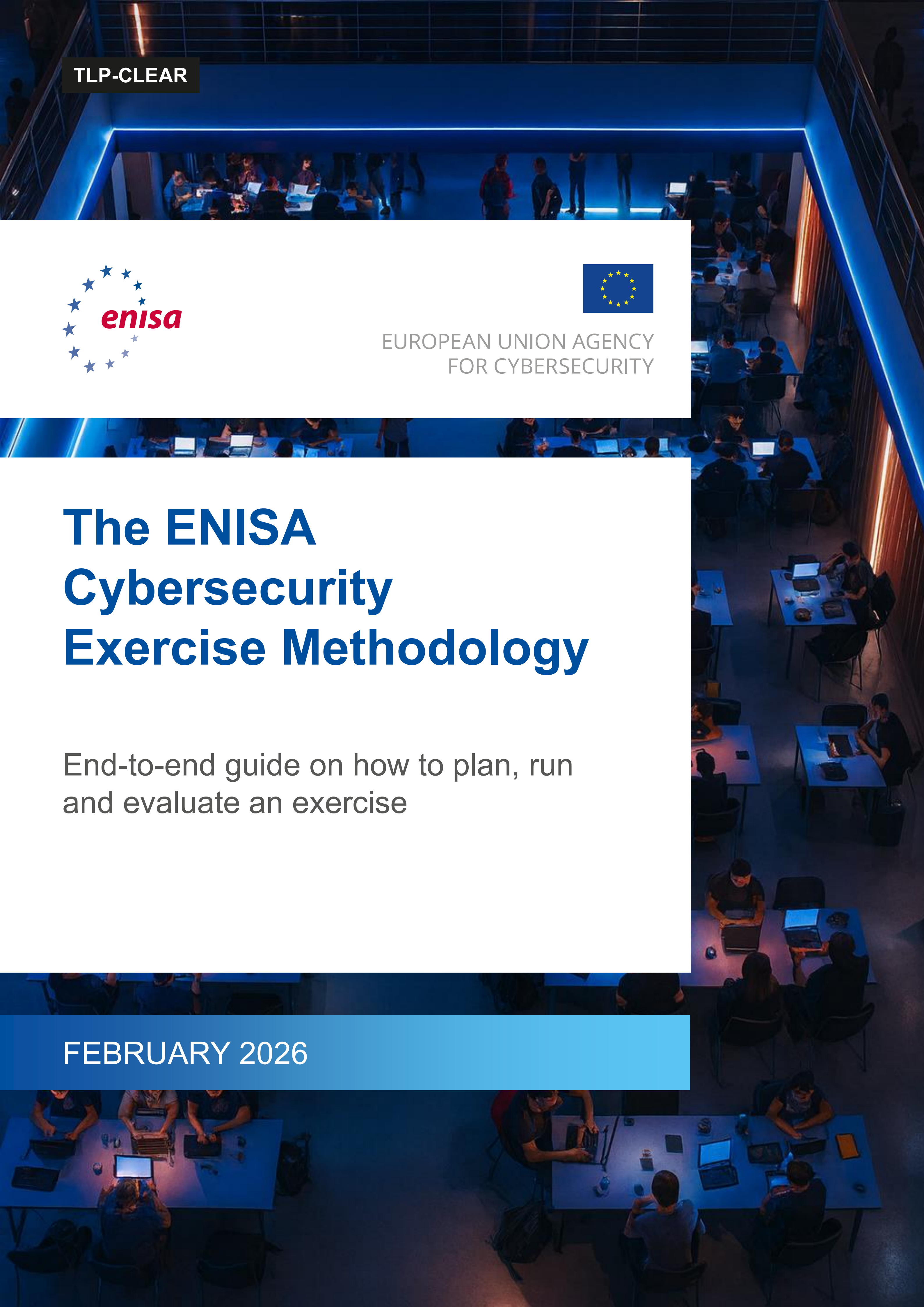


TLP-CLEAR

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

The ENISA Cybersecurity Exercise Methodology

End-to-end guide on how to plan, run and evaluate an exercise

FEBRUARY 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is 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 the 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.

AUTHORS

Alexandros Zacharis, ENISA
Anna Sarri, ENISA
Christian Van Heurck, ENISA
Fanouris Fanourakis, ENISA
Gema Fernández, ENISA
Nikolaos Christoforatos, ENISA
Radu Arcus, ENISA

ACKNOWLEDGEMENTS

Deloitte Belgium

LEGAL NOTICE

This publication represents the views and interpretations of ENISA unless otherwise stated. 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 it must be accessible free of charge. All references to it or its use as a whole or partially must mention 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 978-92-9204-735-1, DOI 0.2824/4949728

TABLE OF CONTENTS

Executive Summary

In today's digital landscape, organisations face increasing cyber threats. Cybersecurity exercises are essential for preparing, testing and enhancing team and system capabilities to respond to these threats. A well-structured cybersecurity exercise methodology ensures a comprehensive approach to simulation and training, building resilience and agility in mitigating cyber risks.

What is the ENISA Cybersecurity Exercise Methodology?

The methodology offers an end-to-end theoretical framework for planning, running and evaluating cybersecurity exercises. It ensures the right profiles and stakeholders are involved at the right time. The methodology provides theoretical material based on lessons identified, industry best practices and cybersecurity expertise, and is designed to be used alongside a support toolkit, including a set of templates and guiding material to empower planners to organise effective exercises.

Who is the methodology for?

The methodology is designed for any cybersecurity professional, organisation or government who wishes to:

- Learn about organising and planning a cybersecurity exercise;
- Assess their current cyberattack response capabilities;
- Convince management of the importance of organising cybersecurity exercises;
- Test skills, response to and resilience against cyber threats, and compliance with legal and regulatory requirements.

Developed and used for EU-level crisis management exercises, the methodology's current focus is ideal for planners organising national or sector-level exercises.

What will the methodology do?

The methodology provides a structured, straightforward approach to planning, running and evaluating exercises, together with a support toolkit to provide practical guidance.

Go/no-go checklists

Go/no-go points between each phase of a cybersecurity exercise life cycle are crucial to ensure all necessary preparations and conditions are met before proceeding. These checkpoints reduce the risk of unforeseen issues, enhance overall effectiveness, allow for timely adjustments and ensure resource allocation aligns with objectives.

Alignment with standards

The methodology is flexible and built to align with established standards like ISO 22398:2013 ([1]) and ISO 22361:2022 ([2]).

Support and community use

ENISA offers resources, regular workshops and a community of cybersecurity experts to support planners. Contact ENISA for workshop schedules and community access.

[1] ISO 22398:2013, Societal security – Guidelines for exercises.
[2] ISO 22361:2022, Security and resilience – Crisis management: Guidelines.

Introduction

What's in it for you?

Testing your organisation's capabilities and its response to and resilience against a cyber crisis is crucial to ensure the right skills, processes and policies are in place. ENISA's documentation makes this process easy and clear with a structured, end-to-end approach:

- **Just fill it in.** The methodology and support toolkit covers all aspects of a cybersecurity exercise. Simply follow the structure and fill in the points relevant to you. This significantly reduces the time you will need for planning compared with starting from scratch, and the comprehensive checklists help eliminate the most common planning oversights. The documentation is designed to be easily understood and communicated across different levels of cybersecurity maturity.
- **Improve and stay compliant.** Identify lessons learned, create an action plan for improvement and ensure your organisation's processes align with relevant regulations and standards. For ENISA's stakeholders, this includes key regulations and directives such as the Network and Information Security Directive (known as NIS2) ([3]), the EU Cybersecurity Act ([4]), the Cyber Resilience Act ([5]), the Digital Operational Resilience Act ([6]) and the General Data Protection Regulation (GDPR) ([7]), and relevant frameworks such as the EU Cyber Blueprint ([8]).
- **Show the value early.** From the start, you will be able to identify at an early stage reasons why your organisation would benefit from running an exercise. The documentation helps you efficiently identify lessons learned and create an action plan to address them.
- **You are not alone.** ENISA offers regular workshops and working sessions to assist planners. You can also access a community of cybersecurity experts for advice and shared experiences.

How it works: core principles

The ENISA Cybersecurity Exercise Methodology guides organisations in developing effective cybersecurity exercises. The principles presented below serve as the foundation for the entire process.

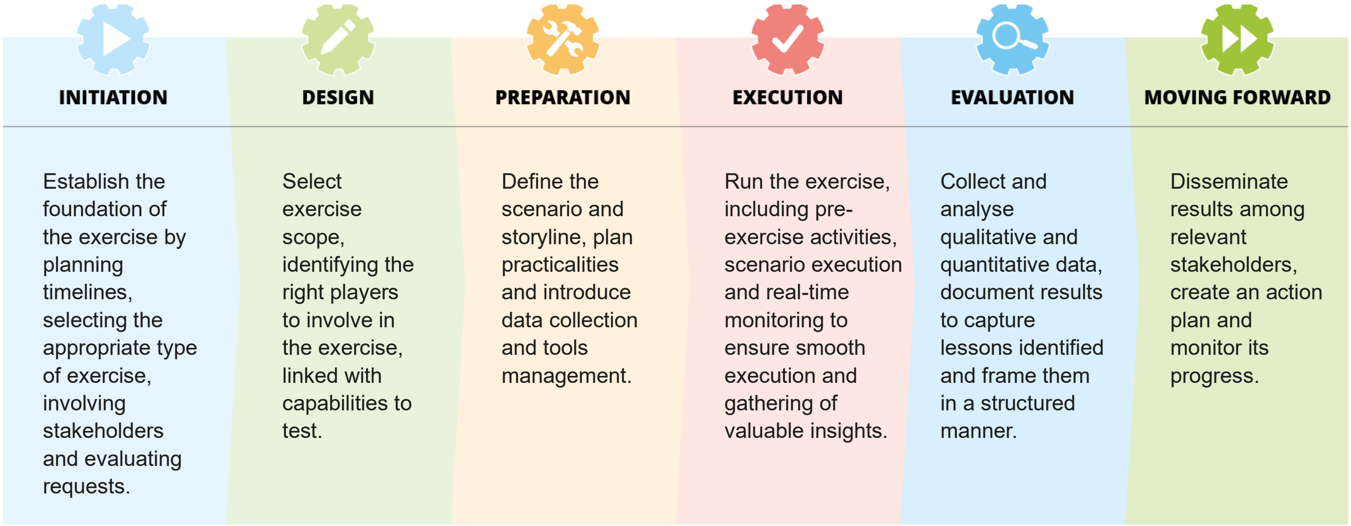
- **Structured planning.** Ensure a systematic, user-friendly, comprehensive approach to designing and implementing exercises. The methodology is designed to make the planning process clear and straightforward, covering all dimensions, including compliance with European regulations and standards.
- **Capacity building**. Systematically assess skills, processes and technologies, identifying gaps and areas for improvement, by setting clear, measurable objectives for effective evaluation and analysis. The methodology is designed to help you efficiently identify lessons learned and create actionable plans, helping your organisation continuously enhance its cybersecurity posture.

[3] Directive (EU) 2022/2555.
[4] Regulation (EU) 2025/37
[5] Regulation (EU) 2024/2847.
[6] Regulation (EU) 2022/2554.
[7] Regulation (EU) 2016/679.
[8] Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management (C/2025/3445).

- **Flexibility**. The methodology is adaptable to organisations' specific needs and maturity level, supporting various exercise types, complexities and sizes. It allows you to easily showcase the benefits of cybersecurity exercises to management and justify the investment.
- **Resources ecosystem**. This theoretical guide for planning, running and evaluating exercises is aligned with, and works together with, the European Cybersecurity Skills Framework and a support toolkit, which includes templates for main exercise documentation and practical checklists to guide you through the process and provide inspiration and insights for your exercise.
- **Community collaboration.** You are not alone in the process. The methodology has been designed following feedback from the exercise planner experts' community and will keep evolving over time to reflect the reality of this community. Regular workshops are organised, where discussion and knowledge exchange are encouraged throughout the exercise expert community.

Phases

The methodology is divided into six key phases to guide organisations in creating effective cybersecurity exercises, ensuring they are realistic, impactful and aligned with organisational goals.



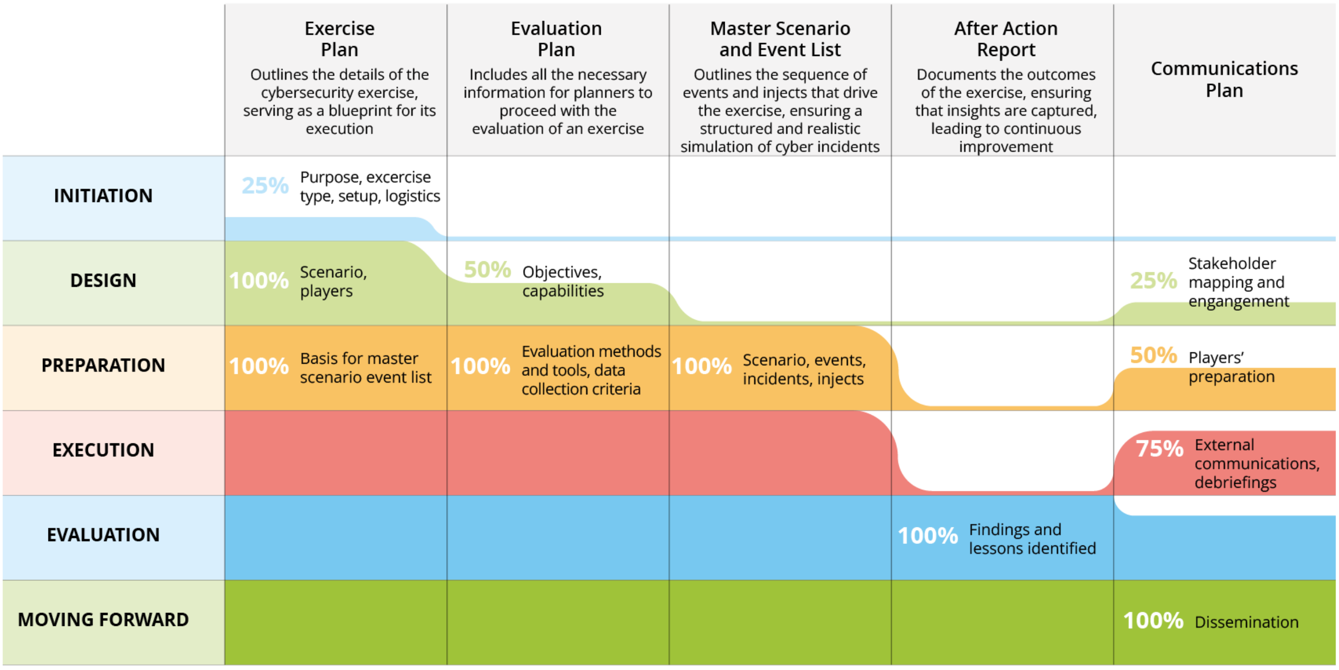
INITIATION	DESIGN	PREPARATION	EXECUTION	EVALUATION	MOVING FORWARD
Establish the foundation of the exercise by planning timelines, selecting the appropriate type of exercise, involving stakeholders and evaluating requests.	Select exercise scope, identifying the right players to involve in the exercise, linked with capabilities to test.	Define the scenario and storyline, plan practicalities and introduce data collection and tools management.	Run the exercise, including pre-exercise activities, scenario execution and real-time monitoring to ensure smooth execution and gathering of valuable insights.	Collect and analyse qualitative and quantitative data, document results to capture lessons identified and frame them in a structured manner.	Disseminate results among relevant stakeholders, create an action plan and monitor its progress.

Figure 1 – Key phases of the methodology

In parallel, the support toolkit provides step-by-step documentation to plan, run and report on a cybersecurity exercise, ensuring organisations can develop, implement and refine effective exercises for improved preparedness for and resilience against cyber threats.

Key deliverables

This methodology helps prepare key deliverables for a successful cybersecurity exercise throughout the exercise-planning life cycle.



	Exercise Plan Outlines the details of the cybersecurity exercise, serving as a blueprint for its execution	Evaluation Plan Includes all the necessary information for planners to proceed with the evaluation of an exercise	Master Scenario and Event List Outlines the sequence of events and injects that drive the exercise, ensuring a structured and realistic simulation of cyber incidents	After Action Report Documents the outcomes of the exercise, ensuring that insights are captured, leading to continuous improvement	Communications Plan
INITIATION	25% Purpose, excercise type, setup, logistics				
DESIGN	100% Scenario, players	50% Objectives, capabilities			25% Stakeholder mapping and engangement
PREPARATION	100% Basis for master scenario event list	100% Evaluation methods and tools, data collection criteria	100% Scenario, events, incidents, injects		50% Players' preparation
EXECUTION					75% External communications, debriefings
EVALUATION				100% Findings and lessons identified	
MOVING FORWARD					100% Dissemination

Figure 2 – Evolution of deliverables along the phases

A complete set of deliverable templates is available in the support toolkit.

The European Cybersecurity Skills Framework

ENISA uses the European Cybersecurity Skills Framework (ECSF) ([9]) to map stakeholders, defining 12 typical cybersecurity professional role profiles. These profiles outline the main missions, tasks and skills needed in a professional cybersecurity context. Using the ECSF ensures common terminology and shared understanding of cybersecurity roles across the EU, enables the identification of critical skill sets required for the cybersecurity workforce, and promotes harmonisation in cybersecurity education, training and workforce development programmes.

This mapping will be used throughout this document to align typical cybersecurity exercise roles with the ECSF.

[9] European Cybersecurity Skills Framework

SECTION 1

Initiation

1. Initiation

DESCRIPTION

This chapter provides guidance on initiating a new cybersecurity exercise project. It determines the project's viability, sets expectations and outlines requirements for later stages.

DELIVERABLES

Initiate the **exercise plan**

STEPS

1.1 - Why do you want to organise an exercise?
1.2 - Choose the right exercise type
1.3 - Define the required resources
1.4 - Assess your cybersecurity posture
1.5 - Assess the feasibility of an exercise

SUPPORT TOOLKIT MATERIAL

Exercise request template

1.1 Why do you want to organise an exercise?

The decision to proceed with a cybersecurity exercise needs to start by understanding the underlying purpose of a cybersecurity exercise for oneself, whether it is at the individual, organisational or governmental level. This is fundamental to achieving meaningful outcomes.

Typically referred to as the goal, the 'why' provides the foundational reason for the exercise, ensuring stakeholder buy-in, motivation and alignment with broader strategic goals. It helps to frame the objectives with the right focus. The central question to address is.

The 'why' is the purpose and mission of the person, organisation or public administration organising an exercise. It is not an objective. While the 'why' outlines the core mission, the objectives define 'how' you will fulfil that mission.

Concise and understandable messages that resonate with a broad audience will motivate stakeholders to actively engage and collaborate, serving as a call to action for the exercise.

Five Whys: supporting technique

The five 'whys' method involves repeatedly asking 'why' to drill down to the core purpose. The following is an example of a sequence.

1. **Why will I participate in Cyber Europe?** To be a part of a pan-European large-scale exercise.
2. **Why?** To test my country's response to a potential cybersecurity threat.
3. **Why?** To make sure the right people have the right skills.
4. **Why?** To ensure they we can detect, respond to, operate and recover from that cybersecurity threat.
5. **Why?** To make Europe safer from cybersecurity threats.

PRO-TIP

Reasons to organise an exercise

- **Risk identification and mitigation:** proactive identification and mitigation of vulnerabilities and gaps in cybersecurity posture.
- **Incident response preparedness:** practice and refinement of response procedures, communication protocols and decision-making via simulated real-world cyber incidents in a controlled environment.
- **Stakeholder collaboration:** enhanced collaboration and coordination among internal and external stakeholders, strengthening collective response capabilities.
- **Continuous improvement:** regular exercises allowing for continuous evaluation and improvement of cybersecurity strategies, policies and procedures based on lessons identified and emerging threats.
- **Compliance and regulatory requirements:** compliance with relevant regulatory frameworks and industry standards.

1.2 Choose the right exercise type

Organisations can employ various types of exercise to test their preparedness for and resilience against cybersecurity threats. These exercises evaluate different aspects of cybersecurity readiness and response capabilities. Planners must choose the appropriate exercise type based on the defined objectives and capabilities. Two examples are given below.

- **Discussion-based exercises:**
  - Focus on collaborative discussions and decision-making;
  - Enhance awareness, understanding and communication of cybersecurity risks, policies, procedures and roles;
  - Explore response strategies to simulated scenarios, emphasising communication and planning without physical deployment.

Example: Discussion-based exercises facilitate interactive discussions to evaluate preparedness, response strategies and decision-making processes.

- **Operation-based exercises:**
  - Test and validate operational procedures, technical capabilities and response actions in a simulated environment;
  - Assess the effectiveness of incident response plans, procedures and technical controls;
  - Are scenario-driven exercises that allow planners to test actual response processes and operational readiness in a simulated but realistic environment.

Example: Operation-based exercises provide an immersive platform to test the practical application of response plans and technical capabilities in simulated scenarios.

When selecting the right type of cybersecurity exercise, planners must ensure that the exercise aligns with their objectives, capabilities and risk profile (see table below).

Table 1 - Decision criteria to choose the right exercise type

Decision Criteria	Discussion-based	Operation-based
Exercise 'whys'/goals	Discuss strategic, policy or procedural aspects without deploying resources.	Test actual response capabilities and operational readiness in a simulated environment.
Target audience	• Political decision makers • Mid to upper-level management	• Response teams • Communication teams • Cybersecurity analysts • More operational stakeholders
Resources and logistics	Suitable when resources are limited; focuses on understanding, communication and coordination. Appropriate when the objective is to limit costs.	Requires more resources to simulate a real-world environment for testing physical and technical responses. Appropriate when a sizeable budget is available.

Readiness level	Ideal for early stages of cybersecurity framework development, reviewing response plans due to changes and assessing applicability to real-world situations.	Used to assess effectiveness in a real-time scenario, testing systems, communication and performance under stress.
Training and awareness	Raises awareness, educates on new threats/policies and improves strategic understanding through discussions.	Trains personnel in specific roles, tests operational procedures and enhances hands-on skills.
Evaluation and improvement	Identifies knowledge and strategic planning without complex logistics.	Provides a comprehensive evaluation of operational effectiveness, identifying technical and procedural improvements.

Exercise planners can select from various types of exercise within the discussion-based category. The table below helps planners choose the most suitable exercise by describing each type, considering specifics like duration, target audience and planning effort required (a minimum of six months for discussion-based exercises).

Table 2 - Different categories of exercises, including exercise type, description and level of interaction

Category	Exercise Type	Description	Level of interaction	Indicative Duration	Effort	Target Audience
Discussion-based	Seminar/ workshop	Formal educational event, focusing on delivering information or insights on a specific topic or research area. It is often lecture based, with the goal of informing or educating the audience.	Low	1-4 hours	Low (< 4 weeks to plan)	Decision makers Mid to upper-level management
	Tabletop	Facilitated interactive session that focuses on building specific skills or knowledge through active participation. It is usually more practical and task oriented, designed to solve problems or develop skills.	Very High	2-8 hours	Medium (4–8 weeks to plan)	
Operation-based	Drill	Focused exercise aimed at testing the effectiveness of a specific part of a cybersecurity playbook, such as incident response to a phishing attack.	Moderate	1-2 hours	High (16 –32 weeks to plan)	Response teams Communication teams Cybersecurity analysts More operational stakeholders
	Game	Competitive, scenario-based activity that simulates cybersecurity incidents to encourage learning through strategy and problem-solving in a controlled, gamified/simulated environment (e.g. a cyber range).	High	2-8 hours	High (8 –16 weeks to plan)	

	Operational	Comprehensive exercise that simulates a real-life cybersecurity incident, testing the organisation's response and coordination across all functions and teams, internal and external. These exercises can be operational, technical or both.	Very High	1- 2+ days	Very high (32+ weeks to plan)	

Organisations can thoroughly assess their readiness by choosing the most appropriate type of exercise based on specific objectives and capabilities. By considering criteria such as objectives, audience and resources, planners can tailor exercises to their needs.

1.3 Define the required resources

Organising a cybersecurity exercise requires careful resource allocation in terms of people, technology, budget and time. Effective resource allocation ensures that the exercise is well supported, realistic and impactful, leading to improved cybersecurity preparedness and resilience.

1.3.1 Exercise stakeholders

The exercise-planning process should involve a diverse group of stakeholders from various organisational functions and external partners, whose involvement typically varies depending on the type of exercise.

Engaging stakeholders can be difficult, especially when it comes to obtaining senior management buy-in and coordinating schedules and priorities. Exercises contribute to overcoming resistance to change, addressing siloed attitudes and fostering a culture of cybersecurity awareness and collaboration; this is why establishing a clear stakeholder mapping early in the initiation phase is crucial to maximise engagement among relevant stakeholders and therefore key to a successful exercise.

To streamline the mapping process for a cybersecurity exercise, the ECSF ([10]) provides a structured reference for relevant professional profiles and their main responsibilities. ENISA uses these 12 profiles to define the missions, tasks and skills needed in a professional context. Using the ECSF ensures common terminology and a shared understanding across the EU, which in turn helps identify critical skill sets and promotes harmonisation in education, training and workforce development programmes. For the purpose of the exercises discussed here, stakeholders ([11]) are divided into participating and non-participating audiences, both of which have vital roles.

Participating Audience

Participating audience members have an active involvement in the exercise life cycle, with specific tasks across the different phases of organising the cybersecurity exercise. They are divided into teams, with specific skills required within each, as presented below.

[10] European Cybersecurity Skills Framework.

[11] This methodology's terminology aligns with ENISA's usage and may differ from common industry terms. A complete list of definitions is in the glossary.

Table 3 – Description of different teams participating in an exercise

Team of planners	
Responsible for the whole organisation of the exercise. They are the main target audience of this methodology.	
Type	Mandatory
Main ECSF-linked roles	• Cybersecurity educator • Chief information security officer (CISO) *For more information see Annex D 'Potential exercise roles mapping with the European Cybersecurity Skills Framework'.*
Tasks	• Launch the exercise organisation process, including requesting relevant authorisation from key stakeholders/decision-makers. • Lead the scenario definition and development, to ensure the scope aligns with the needs of the organisation(s), and the smooth running of the exercise execution, assuming the facilitator role when needed. Technical expertise may be required, depending on the type of exercises, to make the scenario relevant to the latest threats. • Lead the evaluation tasks, including the definition of objectives, data collection methods and evaluation criteria, the monitoring activities during the exercise execution, and the assessment of the exercise and reporting and dissemination of findings. • Designate, prepare and assist players to ensure the best possible exercise experience. They do not take part in the exercise as players. • Take/ensure ownership and act on exercise findings. Designate, prepare and assist players to ensure the best possible exercise experience. They do not take part in the exercise as players • Take /ensure ownership and act on exercise findings.
Team of players	
Actively engaged in reacting and responding to the simulated actions of the exercise scenario execution.	
Type	Mandatory
Main ECSF-linked roles	Most ECSF roles could be part of the team of players, depending on the scope of the exercise. *For more information see: Section 2.3 'Choose the right players' and Annex D 'Potential exercise roles mapping with the European Cybersecurity Skills Framework'.*
Tasks	• Implement all preparations required by planners before the execution of the exercise, such as accessing any preparation material or training. • Take an active part in the exercise execution by reacting and responding to the exercise injects as in reality (i.e. through usual communication channels, in accordance with relevant procedures, collaborating with other exercise players). They follow general exercise guidelines and specific indications from the planners before, during and after the exercise execution. • Provide feedback information requested for the evaluation of the exercise and read/disseminate, as applicable, the exercise after-action report when available.

Team of expert observers	
Provide insights and feedback before, during and after the exercise in line with their expertise, which contributes to the realism of the scenario and the identification of improvement opportunities.	
Type	Mandatory
Main ECSF-linked roles	Most ECSF roles could be part of the team of observers, depending on the scope of the exercise and the need for expert observations to be included. *For more information see Annex D 'Potential exercise roles mapping with the European Cybersecurity Skills Framework'.*
Tasks	• Contribute to the scenario definition, providing expert insights to ensure realism. • Support the evaluation tasks, mainly contributing to the monitoring activities and providing their expert observations and insights. • They can also support the definition of objectives, the assessment of the exercise and the dissemination of findings within their expert communities when applicable.

Non-participating audience

Non-participating audience members do not have an active role in the planning, execution and evaluation of the exercise, but provide important inputs and are the key outcomes consumers of the exercise. They can be categorised as follows.

- **Key decision-makers/stakeholders.** Their main role is to provide a clear vision and oversee the exercise activities. They provide strategic direction, ensure resource allocation and make critical decisions to ensure the exercise's success, such as initiating or approving the exercise activities or ensuring alignment with organisational goals.
- **External visitors.** They are individuals or entities that do not participate directly in the exercise activities, but are key stakeholders for the organisation. Their perspectives, feedback or observations may still be valuable for assessing the exercise's effectiveness and informing the decision-making processes. They contribute greatly to the dissemination process. Some examples are the press, other teams within the organisation's constituency and key partners.
- **General public.** They are not directly involved in the planning the exercise but may be impacted by its outcomes and would like to be informed about them.

1.3.2 Technology and tools

Effective exercise organisation requires providing the necessary technology and tools to simulate realistic scenarios and support the exercise activities. While deploying these tools, we can encounter potential technical limitations, such as issues with infrastructure, data access and network connectivity, which can impact the whole exercise life cycle.

Design and preparation

Technology is at this stage crucial for managing the exercise from a logistical standpoint and crafting the scenario. This includes using project management software to track tasks and timelines, and collaboration platforms for a unified workspace to develop objectives, write injects and design the exercise narrative. These tools ensure the entire planning team coordinates with one another.

Execution

Technology is used in this phase to deliver the simulated scenario to the participants. The tools will depend on the selected exercise type, as follows.

- **Discussion based.** For a seminar-type exercise, basic presentation and collaboration platforms, together with videoconferencing tools, are used to facilitate discussion and present key information. For a tabletop exercise, interactive polling tools or dedicated web applications are deployed to enable real-time collection of participant answers and decisions.
- **Operation based.** Specialised email injection and simulation platforms may be needed to deliver the scenario information to players. Moreover, cyber ranges and virtualised network environments provide a safe, controlled space for participants to engage in hands-on technical challenges. Finally, access to simulated realistic media environments can enhance greatly the realism of the exercise scenario.

Analysis and evaluation

The final phase relies on technology to gather and process data to measure the exercise's success. This involves using data collection tools, such as survey software or specialised web portals, to gather participant feedback. During a technical exercise, logging and monitoring tools can capture exercise activity and actions. It is important to note that, although these tools are used for data collection during the execution, their deployment and configuration must be completed earlier, during the preparation phase.

The collected data can then be used in conjunction with data visualisation and reporting tools to generate comprehensive after-action reports (AARs) that detail the team's performance, highlight key takeaways and inform future improvements.

1.3.3 Budget

Securing an adequate budget is fundamental to the success of a comprehensive exercise, covering all aspects from planning and execution to evaluation and reporting. Gaining buy-in from senior leadership is essential to enable the allocation of the necessary resources.

A strategic approach involves developing a tiered budget proposal that outlines minimum, ideal and optimal scenarios. This allows you to clearly justify costs by delineating between the foundational elements required for a functional exercise, the value-added capabilities that can be introduced with minimal investment, and the strategic enhancements that will deliver a significant difference in impact and fidelity. This proactive financial planning demonstrates foresight and strengthens the case for the requested funding.

1.3.4 Timeline

Crafting and executing a successful cybersecurity exercise requires a well-defined time frame. The duration of the planning and execution life cycle depends heavily on factors like the exercise type, complexity, number of stakeholders and their collective experience. Securing an adequate time frame for thorough preparation, coordination and resource allocation is key to a successful exercise. Planning well in advance allows for the following.

- **Strategic alignment.** Ensures that the exercise is strategically integrated into key

PRO-TIP

For any cybersecurity exercise planned, start preparing a minimum of **six months** in advance of the intended execution date.

broader exercise calendars, from your own organisation's capacity-building programme to those of peer organisations, national/sectoral authorities and European initiatives.

- **Thorough design.** Allows ample time for detailed risk assessments, scenario development and overall exercise design.
- **Resource allocation.** Facilitates the proper allocation of personnel, budget and technology.
- **Adaptability.** Provides flexibility to adjust the plan based on evolving threats or unforeseen organisational changes.

Estimate your planning time frame

We include this formula as a high-level reference to calculate the ideal preparation time (T_P), measured in months:

$$T_P \, (months) = T_{min} + (T_E \times C \times S) / E$$

- T_{min} is a constant minimum preparation time, which we consider to be six months;
- T_E is the duration of the exercise in days (of eight working hours), with a minimum value of 0.5 (half day or less);
- C is the complexity of the exercise (e.g. a scale from 1 to 5, where 1 is a simple seminar and 5 is an operational exercise);
- S is the number of primary stakeholder groups involved (e.g. 1 to 5, where 1 is internal stakeholders only, and 5 includes multiple external partners);
- E is the planning team's collective experience (a value from 1 to 5, where 1 is novice and 5 is expert).

EXAMPLES

1. Two-day national operational exercise (T_E=2) with high complexity (C=5) and multiple external stakeholder groups (S=5) planned by an intermediate team (E=3) would require:

$$T_P = T_{min} + (T_E \times C \times S) / E =$$

$$T_P = 6 + (2 \times 5 \times 5) / 3 \simeq \textbf{23 months}$$

2. A single-day national exercise that is estimated to take six hours (T_E = six hours / eight working hours) or 0.75 days with medium to high complexity (C = 4, operational with technical components) and three main stakeholder groups (Security Operations Centre (SOC) team, IT infrastructure, management) (S = 3) planned by a team that has limited experience (E = 2) would require::

$$T_P = T_{min} + (T_E \times C \times S) / E =$$

$$6 + (0.75 \times 4 \times 3) / 2 \simeq \textbf{10.5 months}$$

1.4 Assess your cybersecurity posture

Before planning your cybersecurity exercise, you need to understand your organisation's current security capabilities and weaknesses – what we call your 'cybersecurity posture'. This assessment helps ensure that your exercise targets real needs rather than assumed ones. For first-time planners this may seem daunting, but we'll break it down into manageable steps.

Starting with a cybersecurity posture assessment is crucial as it provides a baseline understanding, identifies risks and vulnerabilities, aligns stakeholders and quickly identifies areas for improvement. This ensures targeted, relevant and impactful efforts, enhancing cybersecurity resilience and preparedness. Planners can use their existing frameworks or adapt the approach below to their organisation's needs.

A three-step approach to assessing cybersecurity posture

1. General Assessment
   - **Purpose.** Provides a high-level overview of the organisation's ability to identify, respond to and recover from cybersecurity incidents.
   - **Methodology.** Use surveys, interviews and documentation reviews.
   - **Outcome.** Determine overall cybersecurity posture, strengths and weaknesses.
2. Vulnerability Assessment
   - **Purpose.** Identifies specific vulnerabilities within systems, applications and processes.
   - **Methodology.** Perform manual reviews and prioritise findings according to criticality.
   - **Outcome.** Compile a report detailing vulnerabilities and their severity, and prioritise them based on risk level.
3. Gap Analysis and improvement areas
   - **Purpose.** Identifies gaps between current cybersecurity posture and desired standards, recommending areas for improvement.
   - **Methodology.** Conduct compliance reviews, benchmarking, gap identification and root cause analysis, and develop improvement recommendations.
   - **Outcome.** Compile a gap analysis report and identify actions for exercise objectives.

PRO-TIP

- Allow **2-4 weeks** for this assessment
- You will need access to cybersecurity-related documentation and key staff for interviews
- Results will directly inform your exercise objectives (Important to connect it to the exercise planning)

1.5 Assess the feasibility of an exercise

Having understood the cybersecurity posture, the next logical step is to evaluate whether it is feasible to conduct the exercise. This feasibility check acts a reality filter, helping to avoid committing to an exercise that cannot be successfully delivered.

First, you must ensure that your exercise objectives align with your strategic goals, risk management priorities and legal/compliance requirements. It is essential to confirm the relevance of these objectives in addressing current cyber threats and operational needs identified in prior risk assessments, all while ensuring alignment with applicable laws and industry standards.

PRO-TIP

- Build flexibility into your timeline to accommodate adjustments and ensure sufficient time for planning and execution.
- Foster engagement through regular updates and active involvement in the planning process.
- Conduct assessments and testing of systems and infrastructure well in advance to ensure that they are ready for the exercise.

Following this, you need to assess the level of stakeholder engagement and commitment. This includes executive leadership, technical teams and external partners. It is important to identify any potential barriers to their participation and secure their buy-in.

The majority of these barriers are normally linked to the availability of resources; this is why a thorough resource assessment is necessary to evaluate the availability of personnel, budget and external support. This step also covers technical feasibility, ensuring that all required technology, systems and infrastructure are available and compatible for the exercise. You must also consider the proposed timeline and scheduling to confirm that there is enough time for planning, coordination and execution without negatively impacting other operational priorities.

Finally, you should review lessons identified from previous exercises. This helps you to incorporate best practices and identify opportunities for continuous improvement.

By systematically evaluating each of these areas, you can develop a solid plan that is both realistic and effective.

1.6 Deliverables check: initiation phase

Once you have a clear focus and approach to conducting an exercise, collect all relevant information in a single document, the exercise plan, which will serve as the focal point for all decisions moving forward. The exercise plan is critical and must be frequently revised as planning progresses (more information is included in Annex B 'Key deliverables'*)*.

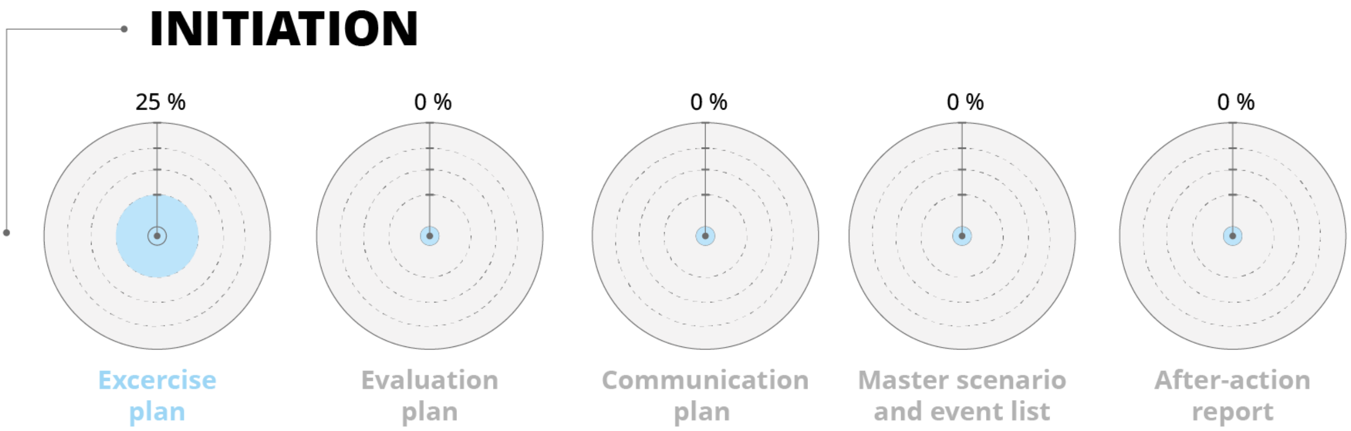


Figure 3 – Deliverable status at the end of the Initiation phase

SECTION 2

Design

2. Design

DESCRIPTION

This chapter provides guidance on structuring and defining the essential aspects of the exercise once its feasibility has been confirmed. It defines the scope, objectives and players.

STEPS

2.1 Define the objectives
2.2 Define the scope
2.3 Choose the right players
2.4 Start communicating about the exercise

DELIVERABLES

Finalise the **exercise plan**
Initiate the **evaluation plan** and the **communications plan**

SUPPORT TOOLKIT MATERIAL

Templates for exercise plan, evaluation plan and communication plan

2.1 Define the objectives

After establishing your exercise purpose (the ‘why’ from the initiation phase), you must define clear, measurable objectives that specify what the exercise will achieve.

Setting clear and measurable objectives is crucial for the success of any cybersecurity exercise. Objectives should align with the organisation’s strategic goals and reflect its key performance indicators, ensuring that the exercise is relevant and capable of driving meaningful improvements. Well-defined objectives ensure focus and clarity, whereas poorly defined ones can lead to inefficiency and missed learning opportunities.

Objectives are often defined using the SMART framework, meaning they are specific, measurable, achievable, relevant and time bound. These objectives may include enhancing incident response capabilities, testing resilience against specific threats or improving coordination among stakeholders.

PRO-TIP

Smart Objectives

- **Specific**. Target a precise capability or process.
- **Measurable**. Include clear success criteria.
- **Achievable**. Realistic within your resources and time frame.
- **Relevant**. Directly linked to identified risks or requirements.
- **Time bound**. Accomplished within the exercise duration.

For the scope of this methodology, ENISA has derived a set of objective themes to serve as inspiration and guidance. These themes are derived from applicable EU policies such as the NIS2 Directive, the Cybersecurity Act and the EU Cyber Blueprint. They are as follows.

- **Strategic.** High-level objectives that align with the organisation’s overall strategy and long-term vision.
- **Operational.** Specific tasks and activities that need to be performed during the exercise.
- **Human factors.** Human elements of cybersecurity, including awareness, training and behaviour.
- **Process improvement.** Identify and improve existing processes and procedures.
- **Business continuity.** Ensure the organisation can continue operations during and after a cybersecurity incident.
- **Compliance and legal.** Ensure adherence to legal and regulatory requirements.

A table with more detail on objective themes is included in Annex C ‘From objectives to capabilities’. Finally, add detail to your chosen themes by addressing the following three important questions.

- **What do you want to achieve?** Define the desired outcome as precisely as possible, including the systems, tools and methodologies involved.
- **Who is targeted?** Identify the specific individuals, roles or teams responsible for achieving the objective.
- **What is the measure of success?** Define the expected outcomes and how you will measure whether the objective was met.

SAMPLE OBJECTIVES

- Demonstrate compliance with NIS2 incident reporting requirements within mandated time frames.
- Test the incident response team's ability to detect and contain a phishing campaign within two hours.
- Verify cross-team and cross-organisation communication protocols during a supply chain compromise.

2.2 Define the scope

Establishing a clear scope is the critical first step in defining an exercise. The scope sets specific boundaries, ensuring that the exercise remains focused and preventing mission drift. This approach guarantees resource efficiency and helps achieve the predetermined objectives.

Building on the analysis from the initiation phase, you can define the scope across key dimensions: the systems and infrastructure to be tested (e.g. production environments, cloud services and third-party systems); the organisational boundaries to be included (e.g. specific departments, geographical locations and external partners); the threat scenarios to be simulated (e.g. types of attacks, threat actor profiles and attack vectors); and the time and operational constraints (e.g. exercise duration and any blackout periods).

To effectively define the scope, it is recommended to follow a structured approach, as follows.

PRO-TIP

When to revisit the scope

- New critical vulnerabilities emerge.
- Organisational structure changes.
- Resources significantly increase or decrease.
- Initial planning reveals unforeseen dependencies.
- Stakeholder feedback indicates critical gaps.

01

START WITH OBJECTIVES

Map each objective to specific systems, teams and processes that must be involved. If testing incident response to ransomware, identify which critical systems would realistically be affected.

02

IDENTIFY DEPENDENCIES

Document system interconnections, data flows and team handoffs. A payment system test may require including the database team, network team and customer service.

03

APPLY CONSTRAINTS

- Resources: budget, personnel, time
- Technical: system availability, maintenance windows
- Business: acceptable risk levels, regulatory requirements
- Safety: what MUST remain operational

04

DOCUMENT EXCLUSIONS

Explicitly state what is OUT of scope:

- 'Production customer databases will not be accessed'
- 'No actual malware will be deployed on live systems'
- 'Physical security testing is excluded'

05

VALIDATE FEASIBILITY

Review the scope against available resources. Can you realistically simulate the identified scenarios with your budget and timeline?

Figure 4 – Process to effectively define scope

Even with a structured approach, exercises can fail due to common pitfalls in scope definition. To ensure your exercise's success, it is important to be aware of and proactively avoid these common challenges. The table below outlines common scope pitfalls, their potential impact and practical solutions for mitigation.

Table 4 - Common pitfalls when defining the scope

Pitfall	Impact	Solution
Too broad *"Test everything"*	Diluted results, resource exhaustion, unclear objectives	Focus on two or three critical processes or systems per exercise
Too narrow *"Test only email server"*	Missing interdependencies, unrealistic isolation	Include connected systems and dependent processes
Undefined boundaries *"Vague participant list"*	Confusion, missing stakeholders, incomplete testing	Create explicit participant matrix with roles and responsibilities
Unrealistic scenarios *"Nation state attacking small business"*	Wasted resources, irrelevant findings	Align threats with actual risk profile and threat intelligence
Ignoring dependencies *"Testing without key vendors"*	Incomplete response, false confidence	Map all critical dependencies during planning

Remember: a focused, well-defined scope that thoroughly tests a few critical areas provides more value than an overly ambitious scope that superficially touches many areas.

2.3 Choose the right players

Selecting the right participants is crucial for exercise success. Players must represent the actual people who would respond to a real incident, possess the necessary authority to make decisions and have the availability to fully participate. The table below presents potential exercise players associated with the main tasks of the relevant ECSF roles.

Table 5 - Exercise playing teams

Team	ECSF Profile	Tasks linked with Player role
Cybersecurity incident response team	Chief information security officer	• Manage the organisation's response to the simulated cyber incident. • Assure information exchange with external authorities and professional bodies. • Ensure that business continuity and critical functions are protected during the exercise.
	Cyber incident responder	• Analyse, evaluate and mitigate the impact of cybersecurity incidents. Identify cyber incidents' root causes and malicious actors. • In accordance with the organisation's incident response plan, restore functionality of systems and processes to an operational state, collecting evidence and documenting actions taken.
	Digital forensics investigator	• Conduct a simulated forensic investigation to uncover the root cause and scope of the breach. • Provide analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion.
	Cyber threat intelligence specialist	• Analyse simulated threat intelligence feeds to identify malicious actors, their motives and their attack methods during the exercise. • Share relevant information to contribute to situational awareness efforts.
Cybersecurity engineering team	Penetration tester	• Act as a 'red team' member, conducting a simulated attack against the target systems. • Act as a 'blue team' member, defending against the attack.
Cybersecurity Legal team	Cyber legal, policy and compliance officer	• Report simulated incidents in line with legal and regulatory obligations. • Ensure that compliance policies are followed during the response, recommending remediation strategies/solutions to ensure compliance.

Other teams relevant to the broader context of a cybersecurity exercise are the **IT team**, the **communications team**, the **human resources team** and the **executive management**. A complete mapping of the ECSF roles and other potential exercise players outside the ECSF profiles that are relevant to the broader context of a cybersecurity exercise are included in Annex D.

2.4 Start communicating about the exercise

Effective communication is the backbone of successful exercise planning. Starting your communication plan early in the design phase ensures that all stakeholders remain informed, engaged and prepared throughout the exercise life cycle.

The communication plan must:

- Build awareness and buy-in before the exercise;
- Maintain engagement during preparation;
- Ensure coordination during execution;
- Capture feedback after completion.

PRO-TIP

Communicate **early**,
communicate **often**,
communicate **clearly**

A template for the communication plan is included in the support toolkit. In order to start the communication plan, you need to identify the required activities for the design phase, as shown in the table below.

Table 6 - First activities of the communication plan

Purpose	Key components	Practical steps
Ensure that all stakeholders are informed about the exercise objectives and scope, and their roles. It helps secure buy-in and fosters collaboration.	• **Stakeholder identification**. Identify all relevant internal and external stakeholders, including employees, partners, third-party vendors and regulatory bodies. • **Communication plan**. Develop a comprehensive communication plan that outlines the objectives, key messages and preferred communication channels for each stakeholder. • **Early engagement**. Engage stakeholders early in the planning process to ensure their input and buy-in.	• **Initial meetings**. Conduct initial meetings with stakeholders to discuss the exercise objectives and scope, and their roles. • **Preferred channels**. Establish preferred communication channels for each stakeholder, such as email, phone, instant messaging or collaboration platforms. • **Regular updates**. Provide regular updates to keep stakeholders informed about the planning progress and any changes.

2.5 Deliverables check: design phase

Once you have clearly defined the scope of the exercise, the teams and player profiles you need to involve and the capabilities that you plan to evaluate, the exercise plan should be completed and the evaluation plan foundations should be defined (more information is included in Annex B 'Key deliverables').

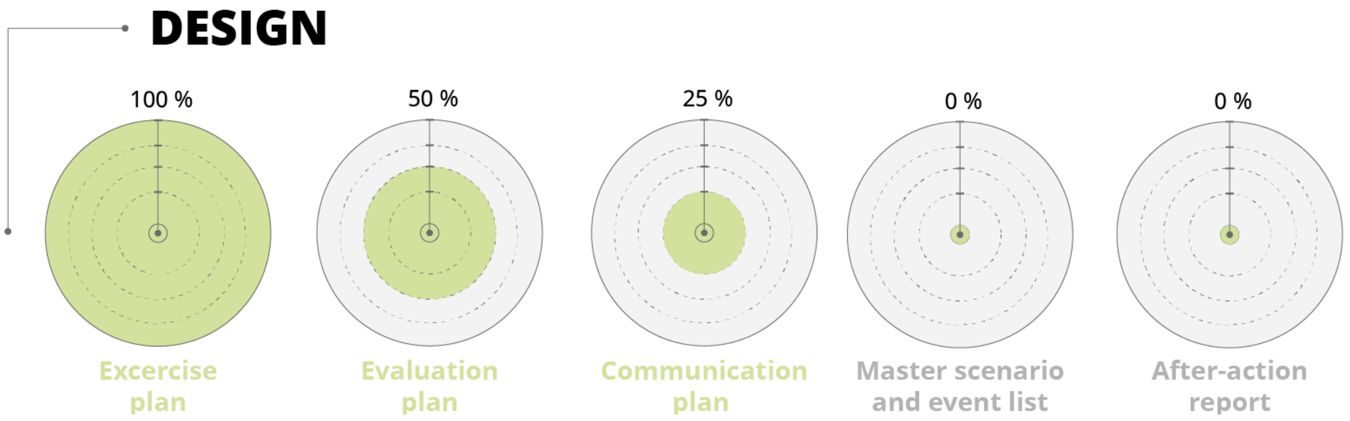


Figure 5 - Deliverable status at the end of the Design phase

SECTION 3

Preparation

3. Preparation

DESCRIPTION

This chapter provides guidance on defining the scenario, planning the practicalities and defining the evaluation criteria, choosing the appropriate data collection methods and tools to capture the data required during the exercise.

STEPS

3.1 Define the scenario

3.2 Define the evaluation strategy

3.3 Prepare the stakeholders

DELIVERABLES

Finalise the **evaluation plan** and the **master scenario event list.** Update the **communication plan**

SUPPORT TOOLKIT MATERIAL

Template for master scenario event list

3.1 Define the scenario

Cybersecurity exercises must be built on realistic and compelling scenarios. The scenario acts as the narrative backbone of the exercise, setting the stage for all activities and decision-making. Developing a successful scenario requires a systematic approach that aligns with the exercise's objectives and reflects the organisation's unique threat landscape.

3.1.1 Main scenario elements

The main elements to define within a scenario are the threat actor(s), the state of the world and the storyline.

Select threats and threat actors

When defining your exercise scenario, it is critical to choose threats and threat actors that are realistic and relevant to your organisation. To do this, you should start by assessing your organisation's specific threat landscape. Some recommendations are as follows.

- **Look at sector-specific threats.** It is good practice to examine the most prevalent threats targeting your sector. This ensures that your exercise is based on realistic and common attack patterns that you are most likely to face.
- **Choose a relevant threat actor.** Based on the type of threat you have selected, you can then choose a plausible threat actor. For example, a ransomware attack may link to a cybercriminal group, while a denial-of-service attack could be associated with a hacktivist, and a more sophisticated, highly targeted attack may correspond to a state nexus group. This helps to make the scenario more realistic and aids in the development of a compelling narrative for the exercise.

The annual ENISA Threat Landscape report ([12]) is a valuable resource. It provides a comprehensive, high-level overview of the most significant cyber threats and trends affecting the EU, offering a solid foundation for your scenario development.

[12] ENISA Threat Landscape.

State of the world: what happened before

The state of the world element sets the context and provides a narrative for the exercise by detailing what has happened in the days or weeks leading up to the scenario's start. This background information is crucial for enhancing realism and helping participants understand the situation.

This section should outline any significant events that are relevant to the exercise, such as:

- previous attacks that may demonstrate the threat actor's capabilities or intent;
- pre-existing conditions, such as a system that has been exhibiting erratic behaviour, which may materialise as a full-blown incident during the exercise (e.g. data exfiltration);
- the broader geopolitical or organisational context that could influence the scenario.

Providing this information in advance helps participants make more informed decisions and ensures that they have a common understanding of the environment and the potential threats they are facing.

Storyline: what will happen during the exercise

The storyline is the narrative that outlines what will happen during the exercise. It serves as the script, guiding the events that unfold in real time and providing context for the participants' actions.

To ensure that the exercise is effective, you must craft a realistic storyline. Your narrative should mimic real-world conditions with a clear timeline of events. The events can be delivered to participants through various injects, such as emails, instant messages or simulated news reports.

While it should be compelling, the storyline should not be overly predictable or excessively dramatic. Avoid information overload, as this can confuse participants and detract from the exercise's primary objectives. Instead, focus on a narrative that is plausible and directly linked to the threats and vulnerabilities identified during the scoping phase.

PRO-TIP

Aim for a balanced scenario

- While it should be compelling, the storyline should not be overly predictable or excessively dramatic.
- Avoid information overload, as this can confuse participants and detract from the exercise's primary objectives.
- Instead, focus on a narrative that is plausible and directly linked to the threats and vulnerabilities identified during the scoping phase.

3.1.2 From storyline to injects

Once the main scenario elements have been clearly defined, planners must translate the overarching storyline into a structured sequence of executable elements. This translation follows a hierarchical framework that ensures logical progression and maintains control throughout execution of the exercise.

Understanding the scenario hierarchy

A cybersecurity exercise scenario operates on three distinct but interconnected levels, each serving a specific purpose in the exercise architecture, as follows:

- **Events** form the highest level, representing major campaign themes or attack patterns that span significant portions of the exercise;
- **Incidents** are specific security breaches or attacks that occur within events, each with defined start and end times;
- **Injects** are the individual pieces of information, prompts or simulated actions, within incidents, delivered to players at precise moments to drive the scenario forwards.

This hierarchical structure enables planners to maintain both strategic oversight and tactical control. Events provide the overarching narrative context, incidents create realistic operational challenges with appropriate duration and complexity, and injects serve as the actual mechanism for scenario delivery and player engagement.

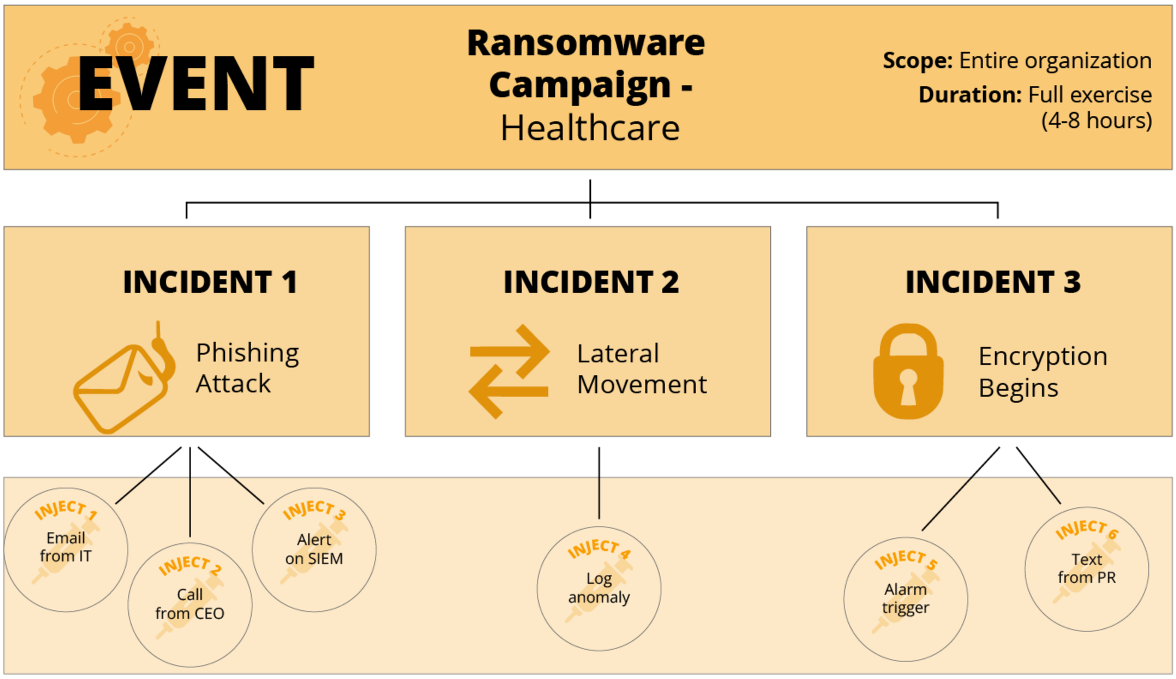


Figure 6 – Hierarchical structure of scenario

Timing and coordination

The temporal relationship between these elements is critical. Events typically run for hours or even the duration of the exercise, providing continuity and context. Within each event, multiple incidents may run sequentially or concurrently, simulating the realistic complexity of cyberattacks. Injects are precisely timed triggers within incidents, delivered through appropriate channels (email, phone call, system alert) to elicit specific responses from players.

The diagram below illustrates how these elements interact within a typical exercise timeline.

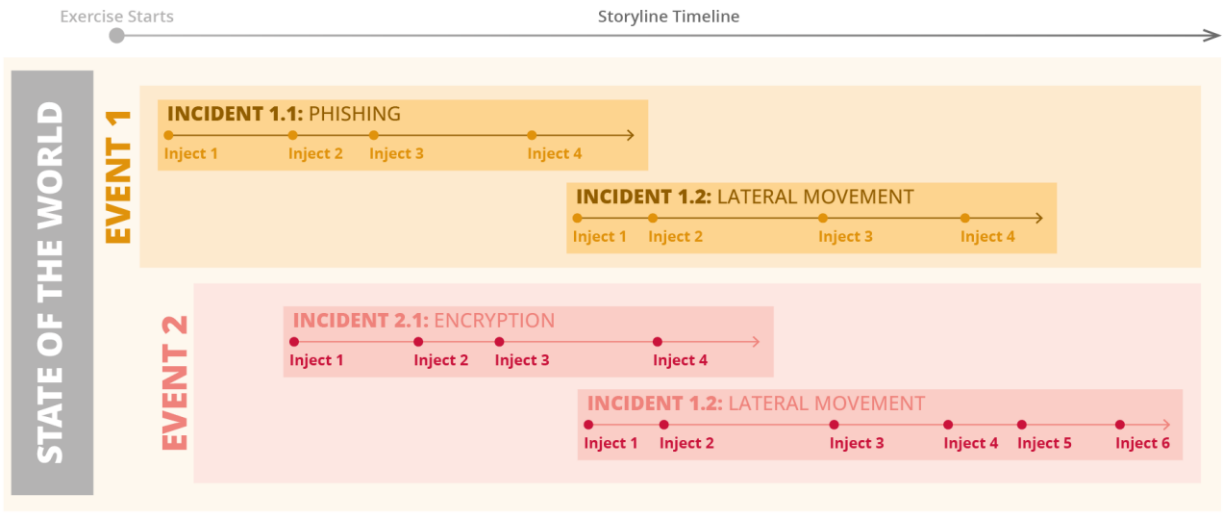


Figure 7 – Chronological structure of the scenario

3.1.3 Master scenario event list

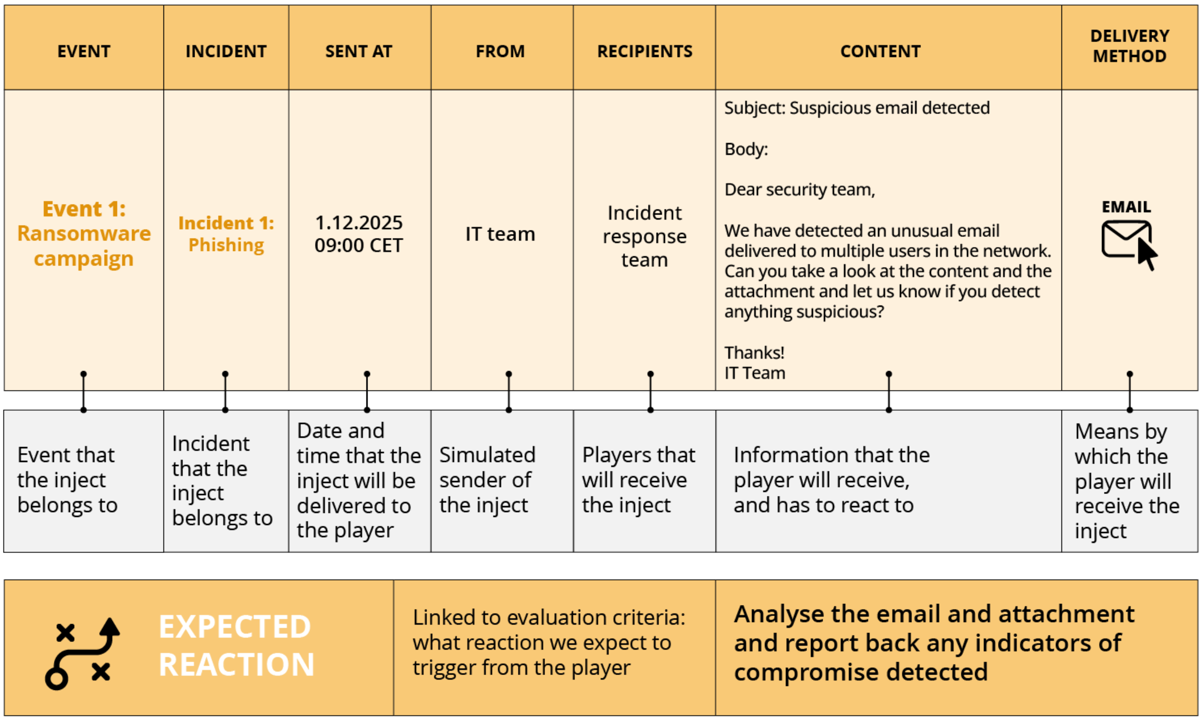
The elements described in the previous subsection are documented in the master scenario event list (MSEL), which serves as the exercise conductor's score. The MSEL is the timeline that guides the exercise control team and the exercise execution automation tools during the execution phase, ensuring that the scenario elements are delivered at the right time to the right people, through the right channels. The MSEL can vary significantly depending on the exercise type, with tailored injects to suit discussion-based or operation-based exercises.

A MSEL template is available in the support toolkit. The table below presents the detail of each technical dimension to define for each exercise scenario.

PRO-TIP

Build a balanced MSEL

- Do not overload participants with too many injects or inject events too rapidly, as this can paralyse response efforts.
- Build critical decision points into the scenario to test risk assessment and decision-making under pressure. Do not make decisions obvious or binary, without real consequences or complexity.



EVENT	INCIDENT	SENT AT	FROM	RECIPIENTS	CONTENT	DELIVERY METHOD
Event 1: Ransomware campaign	Incident 1: Phishing	1.12.2025 09:00 CET	IT team	Incident response team	Subject: Suspicious email detected Body: Dear security team, We have detected an unusual email delivered to multiple users in the network. Can you take a look at the content and the attachment and let us know if you detect anything suspicious? Thanks! IT Team	EMAIL ✉
Event that the inject belongs to	Incident that the inject belongs to	Date and time that the inject will be delivered to the player	Simulated sender of the inject	Players that will receive the inject	Information that the player will receive, and has to react to	Means by which the player will receive the inject

EXPECTED REACTION	Linked to evaluation criteria: what reaction we expect to trigger from the player	Analyse the email and attachment and report back any indicators of compromise detected

Figure 8 – Main elements of an inject

3.2 Define the evaluation strategy

Without proper evaluation, even the best-designed exercise becomes just a training event with no lasting impact. Evaluation transforms your exercise from a one-time activity into a catalyst for real improvement by systematically capturing what worked, what did not and, most importantly, **why**.

In the context of cybersecurity exercises, evaluation means measuring whether the objectives set were achieved, identifying gaps in capabilities or processes and gathering evidence to justify future investments in security improvements.

This section provides a structured approach to designing your evaluation strategy before the exercise begins. By planning your evaluation strategy now (during the preparation phase), you ensure that meaningful data are captured during execution and can be analysed effectively afterwards. This section guides you through defining evaluation criteria (3.2.1), selecting appropriate data collection methods and tools (3.2.2) and preparing stakeholders for their evaluation roles (3.3).

PRO-TIP

For large exercises, establish a **dedicated evaluation team** with a lead and evaluators assigned distinct responsibilities. Position evaluators strategically to gather pertinent data, adjusting staffing levels based on site needs. Exercise planners can also assist in data collection and provide information to the evaluation team.

3.2.1 Define evaluation criteria

Evaluation criteria are essential for assessing the effectiveness of cybersecurity exercises. They provide a structured standard for measuring performance, identifying strengths and weaknesses, and guiding improvements. These criteria serve as benchmarks to ensure that the exercise achieves its objectives and offers valuable insights into the organisation's cybersecurity posture.

The evaluation criteria can be structured as follows:

- **Indicators** (what you measure).
  These are aspects to capture during the exercise, which link back to the defined objectives.
- **Metrics** (how you measure).
  These are qualitative or quantitative measures of the indicators used to evaluate performance. For each indicator, you should define one or more metrics that provide a clear way to measure its success.
- **Data collection** (where the data come from).
  The different methods and tools for collecting data are further described in Section 3.2.2.

The table below shows how the two first elements work together in the evaluation of a phishing-related objective.

PRO-TIP

A good practice is to specify the indicators as part of the **expected actions** of an inject from the player. It is a great way to keep the MSEL connected with the evaluation strategy.

Table 7 - Defining evaluation criteria

Objective	Indicator	Metrics
Enhance the organisation's ability to detect and respond to phishing attacks	Timely detection and reporting of a simulated phishing email	• **Time to detect (quantitative).** The time elapsed between the email being sent and the first report from a participant. • **Reporting accuracy (qualitative).** The quality and completeness of the information provided in the report, such as correctly identifying the malicious link and sender.

Some examples of indicators to keep an eye on during cybersecurity exercises are:

- **Performance** – response time, detection accuracy and recovery effectiveness,
- **Compliance** – adherence to regulations and standards (e.g. GDPR, NIS2 Directive),
- **Communication and coordination** – effectiveness of internal and external communication,
- **Participant engagement** – level of stakeholder engagement and participation,
- **Incident handling** – ability to identify, respond to and recover from simulated incidents.

3.2.2 Select data collection methods and tools

Exercise planners must select the right evaluation methods and tools depending on the exercise type and objectives, and the specific indicators being measured. This selection and overall evaluation assessment should be reflected in the evaluation plan.

The Kirkpatrick model ([13]) helps you evaluate at different depths, from immediate reactions to long-term organisational impact. The model consists of the following four levels.

- **Reaction**. This evaluates participants' engagement with and the perceived value of the exercise.
- **Learning**. This assesses the increase in knowledge and skills acquired by participants.
- **Behaviour**. This examines whether participants apply what they learned to their daily operations.
- **Results**. This level evaluates the overall impact on organisational goals, such as improved performance and enhanced security posture.

To implement the Kirkpatrick model effectively, exercise planners should use appropriate data collection tools tailored to each level. The table below provides an overview of these methods and tools for evaluating a cybersecurity exercise.

Level	Before	During	After
1. Reaction	*Not applicable*	• **Direct observation.** Assess satisfaction, collaboration, communication and stress levels. • **1-on-1 interviews.** Gather initial experiences. • **Debriefing**. Discuss strengths, weaknesses, lessons identified and areas for improvement.	• **1-on-1 interviews.** Capture qualitative feedback on content, format and facilitation. • **Feedback survey.** Collect quantitative feedback from a larger audience.
2. Learning	• **Pre-exercise (self)-assessments**. Tailor the exercise to participants' needs and skill levels and establish current knowledge. • **Knowledge checks**. Ensure understanding of fundamental concepts.	• **Direct observation.** Focus on learning outcomes and performance. • **Expert assessments.** Evaluate performance based on predefined criteria. • **Logs and recording analysis.** Capture system interactions, communication and responses (e.g. replies to email inject, chat logs).	• **Post-exercise (self)-assessments.** Measure achievement of learning objectives and new skills, identify areas for improvement and measure progress. • **Peer review mechanisms.** Learn from each other's experiences. • **Knowledge checks.** Identify areas needing extra clarification.
3. Behaviour	*Not applicable*	*Not applicable*	• **Direct observation.** Evaluate the transfer of learning to the job. • **1-on-1 interviews**. Determine if acquired skills and knowledge are being used and if behaviour has changed.
4. Results	*Not applicable*	*Not applicable*	• **Analytics.** Track participation and performance, providing insights into decision-making. • **Feedback platforms.** Gather additional input to identify strengths and areas for improvement. • **Learning management system platforms.** Track progress in a predefined learning curriculum.

[13] Kirkpatrick model.

Before collecting data using various methods and tools, it is essential to define the types of data to be collected and how each type will be processed. The data typically fall into two categories, depending on the type of tool that is used and the type of metrics being measured.

- **Qualitative data.** Rich, descriptive information that can include text, images and videos. These data capture the depth of human experiences, opinions and emotions.
- **Quantitative data.** Numerical data that can be measured and quantified. These data provide the ability to test hypotheses, measure variables and establish statistical relationships.

Certain tools are better suited to collecting either qualitative or quantitative data, while some can collect both. In order to complete the evaluation strategy, we need to specify how each indicator will be captured.

PRO-TIP

Guidelines for data collection tools

- **1-on-1 interviews.** Balance open-ended and closed questions.
- **Knowledge checks.** Ensure that each question has a clear, single correct answer.
- **Survey questions.** Design surveys with specific, measurable questions for quantifiable results.
- **Direct observations.** Use a standardised checklist to assess participants' application of learned skills.
- **Analytics and reporting.** Implement automated data collection methods to gather objective performance metrics (e.g. response time, accuracy rates) and provide information to the evaluation team.

Following on from our previous example, the table below includes the data collection elements required to capture the defined metrics.

Table 8 - Data collection elements

Objective	Indicator	Metrics	Data collection tool
Enhance the organisation’s ability to detect and respond to phishing attacks	Timely detection and reporting of a simulated phishing email	• **Time to detect (quantitative).** The time elapsed between the email being sent and the first report from a participant. • **Reporting accuracy (qualitative).** The quality and completeness of the information provided in the report, such as correctly identifying the malicious link and sender.	**Logs and recordings.** A report by email from a participant: • email timestamp (quantitative); • content of the email (qualitative).

3.3 Prepare the stakeholders

Effective exercise execution depends on participants understanding their roles, the scenario context and logistical requirements before they arrive. This information should be compiled by the exercise planners in a practical guide targeting the exercise players. It will ensure that all participants start with consistent baseline information.

Preparation during this phase focuses on two critical activities: developing complete and accurate briefing materials, and establishing effective delivery methods that guarantee that participants receive and understand essential information.

3.3.1 Develop the players' guide

The players' guide serves as a reference for all exercise players. It must be completed during the preparation phase to allow adequate review time before the execution of the exercise. The following important information should be included in the players' guide:

- **Exercise overview** – the purpose, objectives and scope of the exercise, including background information players will need in order to understand the specific exercise context (e.g. the state of the world),
- **Roles and responsibilities** – a clear description of what each participant/team is expected to do,
- **Rules of engagement** – boundaries and guidelines (e.g. 'use normal communication channels', 'do not contact real external entities'),
- **Technical requirements** – systems access, credentials and connectivity information,
- **Schedule and logistics** – exercise timeline, location details, breaks and key contacts.

3.3.2 Deliver the information to the players

Selecting appropriate communication methods that ensure that the players have received and understood the information is crucial. These activities should be incorporated into the communication plan developed during the design phase (see Section 2.4), specifying timelines, responsible parties and communication channels for each method. Depending on the complexity, size and nature of the exercise, planners can choose from several delivery approaches, as follows.

- **Written documentation.** Distribute the players' guide and request that players acknowledge they have received and understood the materials. Consider using a simple form or email confirmation to track responses. This creates a record of distribution and helps identify who may need follow-up support. Planners may want to set a deadline for acknowledgement (e.g. one week before the exercise) to allow time for clarification.
- **Briefing and question-and-answer sessions.** These sessions allow planners to provide more detailed explanations about the exercise, and players to ask questions and clarify uncertainties in real time. Briefings can be conducted in person or virtually, and may be particularly valuable for complex exercises or when players are unfamiliar with the exercise format. Consider recording sessions for players who cannot attend or for later reference.
- **Dedicated training sessions.** For exercises requiring specific technical skills or involving complex scenarios, planners may organise hands-on training sessions. These sessions can help players familiarise themselves with tools, platforms or procedures they will use during the exercise. Training sessions are especially valuable for operation-based exercises in which players need to practise technical responses.

Planners may consider combining multiple methods to accommodate different learning styles and schedules. For example, distributing written materials first, followed by a briefing session, allows players to prepare questions in advance. An important aspect to consider is the timely distribution of the required information to the players in order to allow for proper preparation and address any questions raised or clarifications requested by the players after they have reviewed the material.

3.4 Deliverables check: Preparation phase

Before moving to the execution phase, planners should stop to reflect on all the final checks to be done. A full checklist has been added to the support toolkit to facilitate this phase. This list can and should be tailored to your own needs and reality.

Once you have finalised all necessary preparations for the exercise, the exercise plan, the evaluation plan and the MSEL should be ready

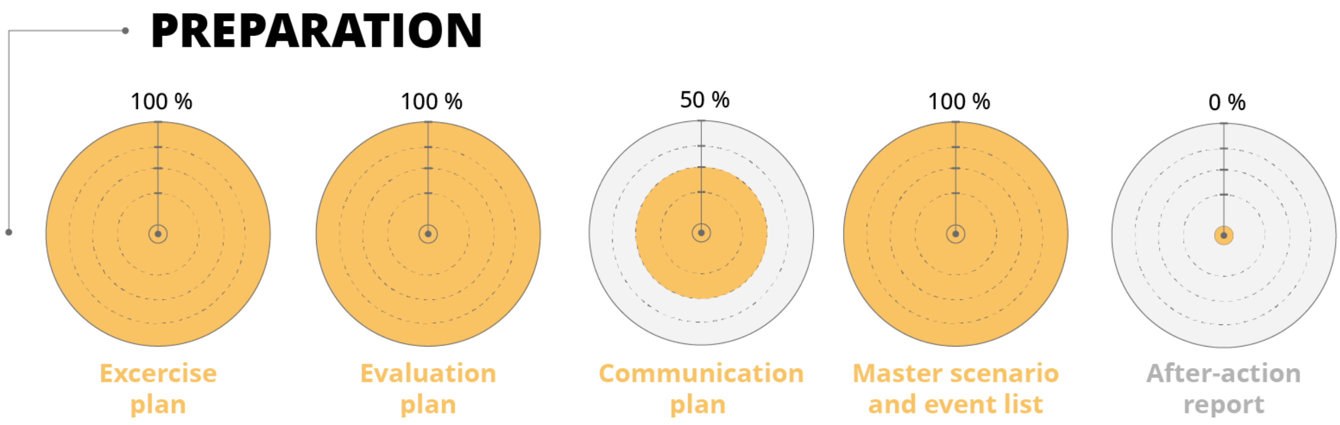


Figure 9 - Deliverable status at the end of the Preparation phase

SECTION 4

Execution

4. Execution

DESCRIPTION

This chapter describes the final steps to execute an exercise, including pre-exercise activities, what to pay special attention to during the execution, and important activities to be performed afterwards to allow for a proper evaluation.

STEPS

4.1 Pre-exercise activities
4.2 Exercise execution
4.3 Post-exercise activities

DELIVERABLES

Update the **Communications Plan**

SUPPORT TOOLKIT MATERIAL

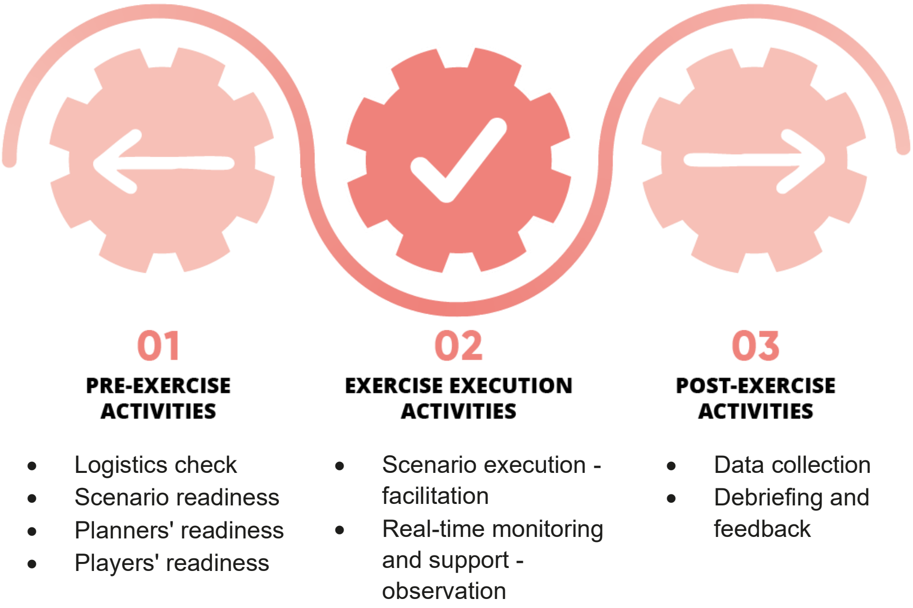
Execution guiding checklists

The execution phase transforms months of planning into action. This is where your scenario comes to life, participants test their capabilities under pressure and evaluators gather critical data for improvement. Success during execution depends on three distinct stages: pre-exercise activities that ensure readiness, the exercise execution itself, when the scenario unfolds, and post-exercise activities that capture immediate feedback while memories are fresh.

This chapter guides you through each stage, highlighting critical checkpoints and common pitfalls. While the support toolkit provides detailed checklists for each activity, this chapter focuses on the strategic decisions and coordination required for smooth execution.

PRO-TIP

Note: the depth of execution activities varies by exercise type. Discussion-based exercises may require simplified briefings and limited data collection, while operational exercises demand full implementation of all components described below



01
PRE-EXERCISE ACTIVITIES

- Logistics check
- Scenario readiness
- Planners' readiness
- Players' readiness

02
EXERCISE EXECUTION ACTIVITIES

- Scenario execution - facilitation
- Real-time monitoring and support - observation

03
POST-EXERCISE ACTIVITIES

- Data collection
- Debriefing and feedback

Figure 10 – Stages for exercise execution

4.1 Pre-exercise activities

Pre-exercise activities represent the critical transition from preparation to action. These final checks, conducted in the hours or days before execution, prevent common failures that can derail even well-planned exercises. Think of this phase as your final systems check before launch – every element must be verified; every participant must be ready and every technical component must be operational.

4.1.1 Logistics check

The primary purpose of this activity is to ensure that the physical environment, equipment and basic infrastructure are operational and ready for immediate use.

Key actions include the following.

- **Venue verification.** Confirm that the venue set-up (e.g. seating, power, internet) is fully complete.
- **Equipment readiness.** Verify that all necessary exercise equipment (e.g. computers, monitors, specialised tools) is in place and functional.
- **Communication channel verification.** Send pre-exercise messages to all registered players before the event begins through the relevant injection channels. This is to verify that players can be reached and identify any issues ahead of time.

PRO-TIP

Dry run versus communication check in operational-based exercises

- A **communication-check** is a test done to ensure that the players can received injects with the method that will be used during the exercise. only one inject is delivered to all players prior to the exercise.
- A **dry-run** is a test the planners organise to refine and validate the MSEL content, simulating the players experience: all injects are delivered to a single location visible only to the planners.

4.1.2 Scenario readiness

Scenario readiness focuses on confirming the robustness of the simulation’s content and ensuring that the exercise control team can manage its flow effectively.

Key actions include the following.

- **MSEL dry runs**. Conduct dry runs of the MSEL to detect any gaps, errors or issues in the injects and timings.
- **Injection material check.** Verify that all scenario-related materials and the required ‘state of the world’ initial conditions are correctly set up.

4.1.3 Planners' and observers’ readiness

During execution, planners can adopt different roles depending on the nature of the exercise, and are considered part of the exercise control team. It is important to ensure that the team is fully organised, briefed and ready to manage the simulation without confusion.

Key actions include the following.

Clear roles and responsibilities

Reconfirm the roles for all exercise control staff (e.g. monitoring, facilitators, expert observers). Each person must understand not just their own role, but how it interfaces with others.

- **Facilitator roles**. Facilitators serve as the primary interface between the scenario and the players. They must be prepared to guide participant actions without leading them to predetermined outcomes, inject scenario elements at precisely the right moments and manage the exercise flow while maintaining scenario authenticity. Conduct a final walk-through of their specific responsibilities: when to intervene, when to let players struggle and how to handle requests that fall outside the exercise scope.
- **Observer roles**. Observers must understand their dual mandate: capture everything while influencing nothing. Brief them on their specific observation points, what behaviours and decisions to document and, critically, when not to intervene – even if players are making mistakes. Their neutrality ensures that the data collected for the AAR remain unbiased and reflect true performance rather than coached responses.

PRO-TIP

The following checks are important **to ensure smooth exercise control** coordination during the execution:

- Can the lead facilitator quickly reach all observers?
- Can technical staff alert facilitators to system issues?
- Can the team collectively decide to adjust the scenario pace without disrupting the exercise flow?

Exercise control coordination

Establish and test the exercise control internal communication and coordination channels and dynamics for real-time management. The final hours before execution should include a complete team briefing in which everyone confirms their understanding of the exercise flow, their individual responsibilities and the communication protocols. This is also the moment to address any lingering uncertainties – better to clarify now than improvise during execution.

4.1.4 Players' readiness

This pre-exercise check ensures that the participation of all players is fully confirmed, and that they understand the rules and possess the necessary information to perform their roles. Key actions include the following.

- **Confirm participation**. Ensure that all exercise players are confirmed and accounted for.
- **Players’ briefing**. Ensure that the players have received and are familiar with key exercise information.

4.2 Exercise execution

4.2.1 Scenario execution

The scenario execution phase focuses on delivering scenario elements (injects) from the MSEL to the players. The method of delivery and the expected player response differ significantly depending on the type of exercise being conducted, but the following are some common activities to be performed to ensure proper scenario execution.

- **Guidance and support.** Provide necessary support and guidance to participants to ensure that they stay within the rules of engagement and work towards the exercise objectives.

- **MSEL delivery.** Systematically deliver scenario injects according to the predetermined timeline of the MSEL.
- **Dynamic adjustment.** Be prepared to adjust the scenario in real time based on unexpected participant actions or responses to maintain a realistic and challenging environment. This includes slowing down or accelerating the pace of injects.

Discussion-based exercises

In discussion-based exercises, facilitators drive the scenario through direct interaction. For this type of exercise, the core activities are analysis, collaboration and decision-making, rather than performing live technical steps. Note the following points.

- The facilitator guides players through the scenario narrative, provides necessary context details and manages the flow of the MSEL.
- Injects are typically formulated as questions (e.g. multiple choice, open ended, structured discussion points), and are designed to trigger analytical debate, strategic decision-making or a coordinated response among playing teams. The responses (discussions, answers or proposed actions) are captured for future analysis.

Operation-based exercises

In operation-based exercises, the focus is on practical, hands-on application of procedures, technical skills and coordination within a simulated environment. They require more complex delivery mechanisms and technical coordination. Note the following points.

- The facilitators ensure that the injects are delivered accurately to the correct audience (e.g. incident responders, system administrators) and through the appropriate means (e.g. simulated email, ticketing system, live network event).
- Injects trigger concrete, measurable actions from the players, such as performing a forensic analysis, communicating with relevant stakeholders or executing a specific technical procedure. Participants are encouraged to follow necessary organisational procedures and protocols. The resulting actions, communications and decisions are captured and logged during the exercise to reflect the result in the AAR.

Technical environment management

During operation-based exercises, maintaining the technical infrastructure is critical for exercise success. This involves the following two parallel responsibilities.

- **Inject delivery systems.** Deploy injects through realistic technical channels appropriate to each player’s role, for example:
  - simulated emails based on the scenario;
  - news items, articles and social media posts on simulated news and social media sites;
  - network anomalies and other technical logs available for analysis;
  - phone calls or video conferences for crisis management.

THE BLUE-ROOM

ENISA’s exercise solution

- The Blue-Room supports cyber exercise projects through all phases, including execution.
- Its implementation is based on modular components adapted to the specific needs of each exercise phase.
- A key feature is the use of a standardised YAML file containing the exercise content

- **Environment integrity.** Continuously monitor and maintain the exercise platform through the following means.
    - System monitoring. Track the health of all simulation components (network connectivity, application availability, data flows) to detect and resolve issues before they impact players (e.g. late or missing inject delivery).
    - Realism preservation. Verify that all technical elements remain consistent with the scenario – ensuring fake events look authentic, simulated malware behaves as expected and system responses match real-world behaviour.
    - Rapid intervention. Maintain a technical support team ready to address any platform issues without disrupting the exercise flow or breaking scenario immersion.

The key is balancing technical complexity with exercise objectives – the environment should challenge players realistically without introducing artificial obstacles stemming from technical failures.

4.2.2 Real-time monitoring and support

During exercise execution, the exercise control team and observers continuously monitor and document participant activities. This real-time data collection is essential for meaningful evaluation and improvement.

Key monitoring activities are as follows.

- **Performance observation.** Document participant actions, decisions and communications against established procedures and expected responses.
- **Event logging.** Record all critical events, player responses and both planned scenario injects and ad hoc exercise control injections with precise timestamps. This comprehensive logging allows accurate reconstruction of the exercise timeline, including any spontaneous adjustments made by the exercise control team.
- **Live feedback capture.** Gather immediate participant insights during scheduled breaks or designated feedback points while experiences remain fresh.

4.3 Post-exercise activities

The post-exercise phase is crucial for ensuring that the investment in the simulation translates into tangible organisational improvements. This phase involves systematic data gathering, participant reflection and structured analysis.

Data collection

Make sure that all the information collected using the methods defined in Section 3.2.2 'Select data collection methods and tools' is properly stored and available for analysis.

Key data to collect and store include the following.

- **Technical records.** Collect all technical logs, network traffic data, communications records (emails, chat transcripts, voice logs) and detailed notes taken by the players and the planners' team during the simulation.
- **Participant feedback.** Distribute structured surveys and feedback forms to participants, observers and facilitators to gather quantifiable input on the exercise's effectiveness, scenario realism and potential areas for improvement.

Structured debriefing

Structured debriefing serves several key purposes in the evaluation of cybersecurity exercises, as follows.

- **Reflection.** Allow participants to reflect on their actions, decisions and outcomes during the exercise.
- **Insight**. Provide valuable insights into the effectiveness of the exercise, including strengths and weaknesses.
- **Improvement.** Identify areas for improvement and guide future enhancements.
- **Engagement.** Foster engagement and collaboration among participants, encouraging open communication and shared learning.

Schedule a debriefing session with all participants to discuss the exercise and provide a complete overview of what happened. Collect feedback from participants, focusing on their experiences, observations and suggestions for improvement.

PRO-TIP

Traditional ways to organise feedback collection

- **Hotwash.** Conduct a feedback session immediately after the exercise where participants can discuss their experiences, challenges and initial thoughts on the exercise while they are fresh in their minds.
- **Coldwash.** Conduct a feedback session some days/weeks after the exercise when participants will have had the time to reflect and process with some distance their experience during the exercise.

The combination of the sessions will give you a complete feedback picture that will allow you to improve future iterations.

4.4 Deliverables check: execution phase

Before finalising the execution phase, planners should ensure that all data have been collected as planned to produce the AAR. A full checklist has been added to the support toolkit to facilitate this phase. This list can and should be tailored to your own needs and reality.

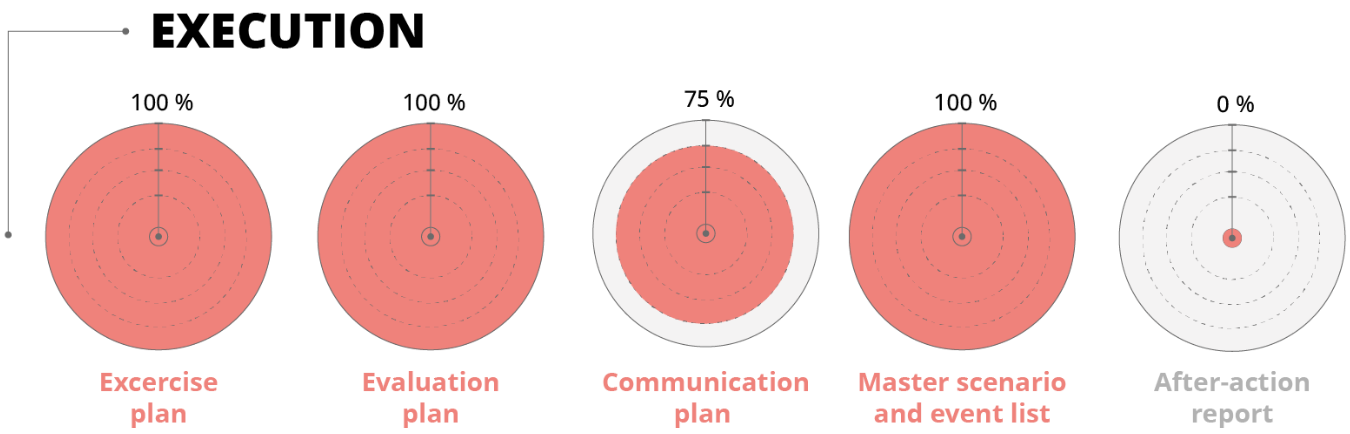


Figure 11 - Deliverable status at the end of the Execution phase

SECTION 5

Evaluation

5. Evaluation

DESCRIPTION

This chapter describes the final steps to evaluate an exercise and ensure data collected from the exercise are transformed into actionable findings. Different techniques to evaluate data collected are proposed and essential aspects to include in the After-action report are identified.

DELIVERABLES

Finalise the **After-action report**

STEPS

5.1 Analysis and assessment

5.2 Reporting

SUPPORT TOOLKIT MATERIAL

After-action report template

5.1 Analysis and assessment

The analysis and assessment phase transforms raw exercise data into actionable findings. This phase answers three critical questions: Did we meet our objectives? Where did we fall short? What caused these gaps? Without rigorous analysis, even the best-executed exercise becomes just another training event with no lasting impact.

As noted in Section 3.2.2 ‘Select data collection methods and tools’, these data typically fall into two categories: qualitative and quantitative. Since using a variety of evaluation tools can generate a large amount of raw data, evaluators must apply different techniques based on the data type. The following sections detail these techniques for extracting valuable insights from the collected data.

5.1.1 Techniques to analyse qualitative data

Qualitative data from exercises – interviews, observations and debriefs – contain rich insights that require systematic analysis. The following three techniques work together to extract meaningful findings.

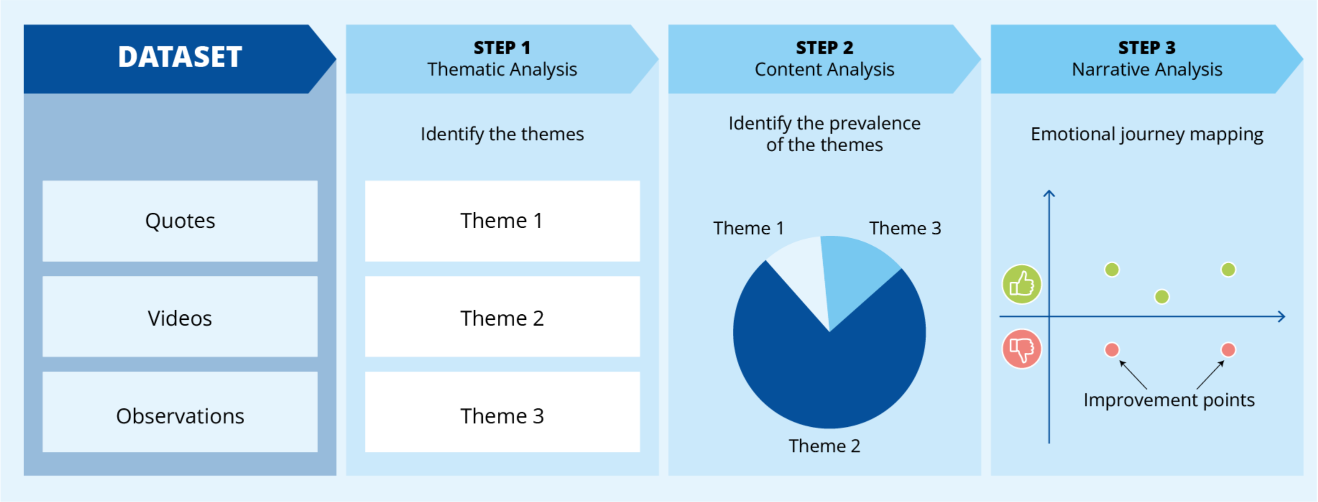


Figure 12: Structure of analysis techniques

Step 1 - Thematic analysis (pattern discovery)

What it does	**Identifies recurring patterns across all qualitative data**
How to apply it	• Read through all observation notes, transcripts and feedback; • Tag recurring topics (e.g. 'communication delays', 'unclear procedures'); • Group similar tags into themes; • Count frequency to prioritise issues.
Example output	*'Communication breakdown' appeared in 73 % of observer notes*

Step 2 - Content analysis (quantifying themes)

What it does	**Converts qualitative observations into measurable data**
How to apply it	• Count specific mentions of each theme; • Track context (when, where, who mentioned it); • Create frequency tables.
Example output	*'Escalation procedures' mentioned 47 times, primarily during incident response phase.*

Step 3 - Narrative analysis (understanding experience)

What it does	**Captures the human story behind the data**
How to apply it	• Examine how participants describe their experience; • Look for emotional indicators and decision-making patterns; • Identify turning points in the exercise flow.
Example output	*Players consistently described feeling 'overwhelmed' at the two-hour mark when multiple incidents converged.*

These three techniques build on each other: thematic analysis reveals what happened, content analysis shows how often it happened and narrative analysis explains why it happened. Together, they transform qualitative observations (see figure above).

5.1.2 Techniques to analyse quantitative data

Quantitative data from your exercise – response times, success rates and compliance scores – tell a numerical story about performance. However, raw numbers alone do not provide insights. You need appropriate analytical techniques to transform data into actionable findings.

The table below presents three statistical approaches, progressing from basic to advanced. Choose techniques based on your evaluation questions and available data. The table includes descriptions of these methods and provides example insights.

PRO-TIP

Selecting the right analysis technique

Before diving into statistics, ask yourself these questions

- What questions am I trying to answer?
- What type of data do I have (counts, times, percentages)?
- How much data have I collected?
- What level of statistical expertise is available?

Table 3: Techniques to analyse quantitative data

Technique	Purpose	When to use	Example application
Descriptive analysis	Describes the main features of a dataset in quantitative terms, allowing you to understand what happened during the exercise	This is the first step for all quantitative data	• Measuring the average time taken by response teams to detect and respond to incidents • Determining the range of scores achieved in different tasks • Identifying the standard deviation in the effectiveness of response strategies across teams
Chi-square test	Determines whether there is a significant association between two categorical variables	These tests reveal whether observed differences between groups are meaningful or just random chance	• Measuring the impact of prior training on performance by comparing the success rates of teams or individuals with different levels of training • Examining the relationship between the type of cyber incident and the likelihood of it being correctly reported to the relevant authorities or internal management • Investigating whether the complexity of the cyber incident affects the success rate of incident resolution
Regression analysis	Examines the relationship between a dependent (target) variable and one or more independent (predictor) variables, helping you understand what factors predict success	This is for when you need to understand cause-and-effect relationships between variables	• Determining how the allocation of resources impacts the efficiency and effectiveness of incident resolution • Modelling how various factors like the complexity of the attack, the number of simultaneous incidents and the team's experience level predict the time taken to detect cybersecurity incidents • Analysing how different response strategies (independent variables) affect the success rate (dependent variable) of mitigating cybersecurity threats

Using these techniques to process the quantitative datasets stemming from the evaluation tools ensures a comprehensive understanding of performance, identifies areas for improvement and informs strategic decisions to enhance cybersecurity resilience.

PRO-TIP

Common pitfalls to avoid

- Overanalysing small datasets (fewer than 30 data points)
- Confusing correlation with causation
- Ignoring practical significance for statistical significance
- Using complex analyses when simple ones would suffice
- Remember: the goal is not to use the most sophisticated technique, but to extract meaningful insights that improve future exercises and cybersecurity readiness.

5.2 Reporting

The AAR helps move from evaluation findings to actionable improvements. This involves meticulously documenting outcomes, insights and recommendations to ensure clarity, accuracy and relevance for all stakeholders.

The AAR uses the traffic light protocol (TLP) to control information distribution, ensuring sensitive findings reach only appropriate audiences.

- **Red:** the AAR is not for disclosure and is restricted to participants only.
- **Amber:** the AAR is for limited disclosure, restricted to participants' organisations.
- **Green:** the AAR is for limited disclosure, restricted to the community and not to be shared through public channels.
- **Clear:** the AAR's disclosure is not limited and it may be distributed with no restrictions, subject to standard copyright rules.

An AAR is a structured document outlining the critical aspects of a cybersecurity exercise. It identifies strengths and weaknesses and informs the audience about required improvements to be implemented. The structure varies based on the TLP type and organisational goals. Typically, an AAR includes the following parts:

- **Executive summary.** This section provides a brief overview of the organisation, as well as a summary for senior management, highlighting key findings and strategic recommendations.
- **Exercise overview.** This part documents essential information, including the exercise's name and date, its scope, core capabilities, objectives, the scenario employed, participating organisations and points of contact.
- **Methodology.** Here, the format of the exercise (i.e. the type of exercise, the evaluation criteria, the data analysis methodology) is described, along with a list of tools, software and technologies utilised during the exercise.
- **Findings and lessons identified.** This part documents the most critical lessons identified from the cybersecurity exercise, including key findings and takeaways.
- **Moving forward.** Recommendations for future iterations are provided here to address the gaps identified during the exercise. This includes specific, actionable suggestions to rectify the weaknesses uncovered.

Internal AARs (TLP red and amber) should include detailed evaluation sections with performance metrics and achievement ratings, while external versions (TLP green and clear) should provide summarised findings to protect sensitive information.

Regardless of TLP classification, the AAR's length and detail level will reflect the exercise's complexity and scope. A sample AAR template is included in the support toolkit.

5.3 Deliverables check: evaluation phase

At this stage of the process, the evaluation phase is finalised, resulting in a complete and action-oriented AAR.

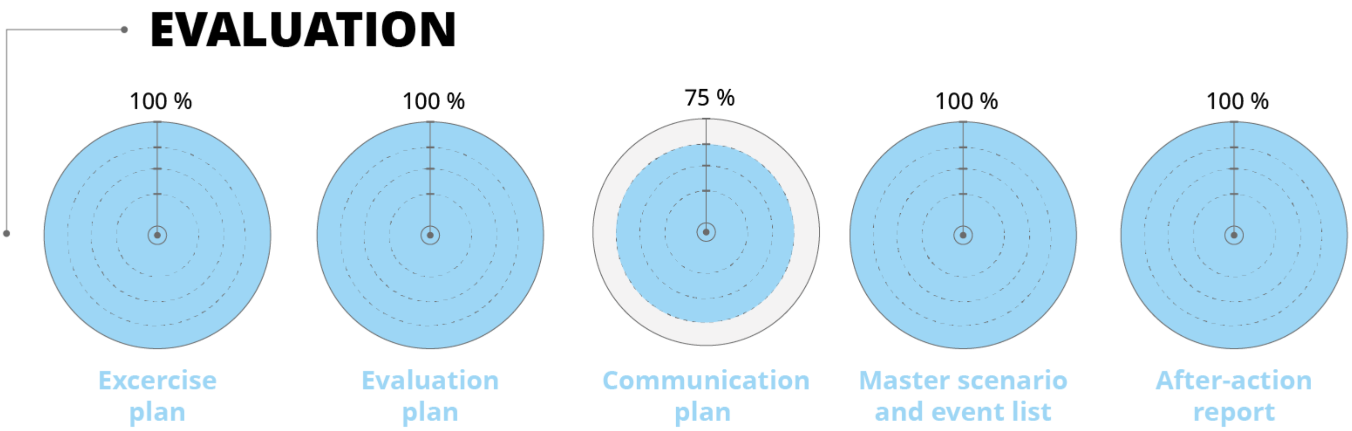


Figure 13 - Deliverable status at the end of the Evaluation phase

SECTION 6

Moving Forward

6. Moving Forward

DESCRIPTION

This chapter describes the crucial process of acting upon the findings of the exercise, from both an organisational improvement perspective and a capacity-building programme angle. The dissemination of the results is also highlighted

STEPS

6.1 Disseminate the exercise results

6.2 Act on the findings

DELIVERABLES

Finalise the **communication plan**

SUPPORT TOOLKIT MATERIAL

Template for action plan

6.1 Disseminate the exercise results

Effective dissemination of exercise results transforms a one-time event into lasting organisational improvement. Without proper dissemination, valuable insights remain confined to a small group, limiting the exercise's impact and return on investment.

Findings and insights from the AAR should inform future actions and strategies; organisations should use these findings to develop action plans to mitigate vulnerabilities, refine policies, enhance training and allocate resources efficiently. Therefore, dissemination serves three critical purposes:

- **Accountability** demonstrates to stakeholders that resources were well spent and objectives were met;
- **Learning** shares lessons across the organisation to prevent future incidents;
- **Action** creates momentum for implementing recommended improvements.

Successful dissemination requires tailoring your approach to each audience's needs, interests and preferred communication channels. Some key audience to reach and the specific objectives for disseminating results with them are as follows.

- **Exercise players.** Understand their performance and areas for improvement.
- **Exercise planners.** Learn from results to enhance their planning skills.
- **Exercise observers.** Identify gaps and provide constructive feedback.
- **Rest of the organisation.** Increase awareness of cybersecurity risks and mitigation strategies.
- **Press.** Report outcomes and educate the public on cybersecurity awareness.
- **General public.** Stay informed about cybersecurity threats.
- **Management board.** Convince investors of the exercise's value and the importance of investing in cybersecurity.

The following table presents appropriate dissemination tools for each stakeholder group, helping planners select the most effective communication methods. These tools should be incorporated into the communication plan started during the design phase.

Table 4: Stakeholders and dissemination tools with their descriptions

Audience	Audience type	Dissemination tool	Description
All	**Combination**	Clear AAR	Documentation capturing exercise events, lessons identified and improvement recommendations.
Participating audience	**Exercise players**: • cross-functional teams • technical teams • departmental teams • remote teams	Briefings and debriefings	Structured meetings before and after the exercise, in which objectives and outcomes are discussed, and feedback is given for next steps.
		Workshops	Interactive sessions with a deep dive into exercise findings and recommendations.
	Exercise planners	Amber AAR	Documentation capturing exercise events, lessons identified and improvement recommendations only for planners.
		Intranet	Platform where posts are regularly put to ensure engagement with and awareness of the exercise results.
		Internal reports	Detailed reports tailored to specific departments, focusing on relevant findings and actions to take.
	Exercise observers	Webinars and online presentations	Virtual sessions for sharing the findings with a broader audience, allowing engagement and questions.
Non-participating audience	Rest of the organisation	Case studies	Analysis of specific exercise incidents or scenarios, which offers them insights into the decision-making process and lessons identified.
	Press	Infographics	Visualisations summarising key exercise data, findings and recommendations.
	General public	Social media posts and website	Sharing insights and best practices through social media to promote awareness and continuous improvement.
	Management board	Executive summary	High-level overview focusing on key findings, business impact and strategic recommendations for the management board.

6.2 Act on the findings

The final step in the exercise life cycle is transforming the raw data from the AAR into concrete, measurable improvements. This process requires action on the following two types of primary, interconnected post-exercise findings that are critical for enhancing both organisational resilience and the quality of future exercises.

- **Findings linked to the exercise objectives.** These findings identify weaknesses, gaps and failures in the organisation’s capabilities, processes or technologies tested during the scenario. Corrective actions here aim to fix the root cause of the security problem.
- **Findings linked to the exercise execution experience.** These findings relate to the quality and efficiency of the exercise itself, such as clarity of roles, timeliness of injects or communication issues between players and the exercise control team. Actions here aim to improve future iterations of the exercise.

Both types of findings directly influence the organisation’s capacity-building programme. Action may involve introducing new training activities to address skill gaps or modifying existing activities to enhance participant effectiveness and learning outcomes.

THE IMPACT ON THE CAPACITY BUILDING PROGRAM

A common and critical action point resulting from both streams of findings is the dynamic update of the organisation's capacity-building programme.

- **Objective-linked findings:** If the findings reveal a skills or capability gap, new training events or capacity-building activities must be immediately included in the programme.
- **Experience-linked findings**: These lessons should lead to changing the approach to how exercises are planned, conducted and evaluated across the entire portfolio of capacity-building activities.

Additionally, once corrective actions (including new training) have been implemented, a replay of the exercise is a best practice for testing the effectiveness of these fixes. This replay should also be included in the capacity-building programme planning.

To systematically address both types of findings, organisations should follow a structured approach.

Steps to create an effective action plan

Following the identification of findings across the two streams (exercise objectives and exercise experience), the next crucial stage is to develop and execute an action plan. This plan incorporates all necessary corrective actions and improvements, ensuring that they are efficiently managed and ultimately successful in enhancing organisational resilience and the quality of the capacity-building programme.

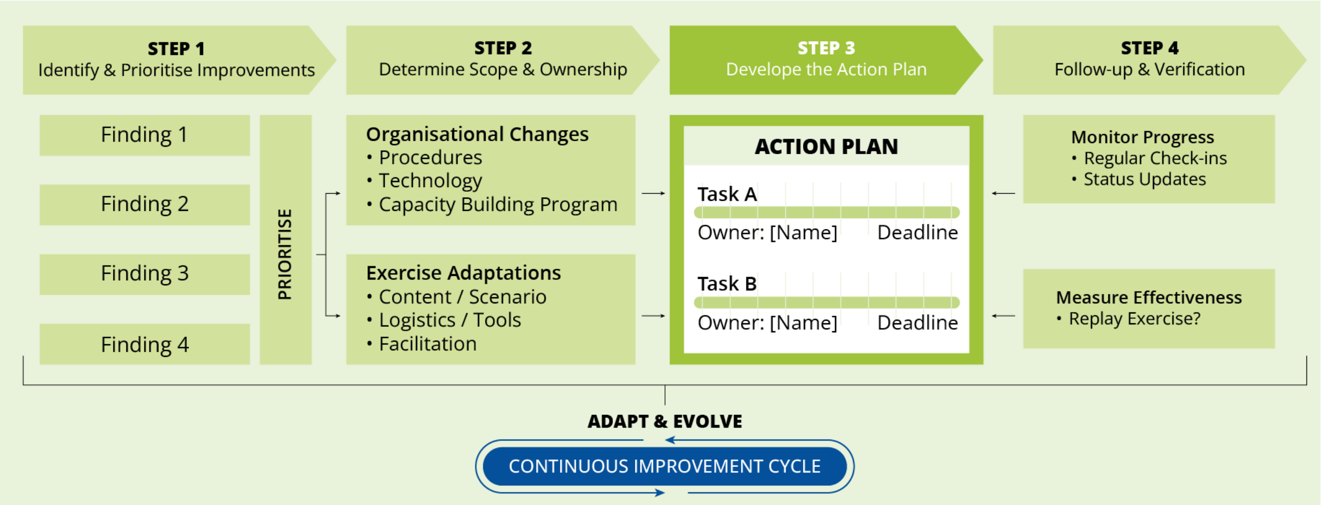


Figure 14 – Steps to create an effective action plan

Step 1: Identify and prioritise improvements

This initial stage involves systematically reviewing all findings from the AAR and feedback sessions, and then prioritising them based on impact and urgency.

- Review findings. Consolidate all identified weaknesses, gaps and areas for improvement from the AAR and feedback sessions.
- Prioritise actions. Evaluate each finding based on its impact, severity and ease of implementation. Prioritise actions considering factors such as criticality, quick wins and strategic alignment. This will result in an ordered list of improvements to address.

Step 2: Determine scope and ownership

Once prioritised, each improvement needs a clear scope and a responsible party to drive its resolution.

- Define scope of action. Classify each improvement according to its primary purpose.
  - Organisational changes. Actions focused on fixing root causes, such as updating procedures, implementing new technologies or adjusting capacity.
  - Capacity-building programme adaptations. Actions focused on improving skills and readiness, such as planning new training events or improving the quality and efficiency of future exercises.
- Assign ownership. For every action item, clearly designate an owner who will be responsible and accountable for its progress and successful completion (for complex initiatives, consider using a ‘RACI’ (responsible, accountable, consulted and informed) matrix to define roles).

Step 3: Develop the action plan

This step converts prioritised improvements into a concrete implementation plan with clear timelines and responsibilities.

- Outline specific tasks. Break down each improvement into manageable, specific tasks required for implementation.
- Agree on deadlines. Set clear and realistic deadlines for the completion of each task.
- Create the plan. Document all tasks, owners and deadlines to form a verifiable roadmap for implementation.

Step 4: Follow-up and verification

This is the ongoing step to ensure that planned actions are actually implemented and that their effectiveness is verified, preventing actions from being forgotten.

- Regular follow-ups. Conduct periodic reviews to monitor the progress of all action items against their established deadlines and ensure that owners are consistently driving implementation.
- Measure effectiveness. Evaluate whether the implemented actions have achieved their intended improvements (e.g. through a subsequent exercise replay).
- Adapt and evolve. Adjust the approach based on observed results and evolving circumstances, ensuring that the organisation's security posture and exercise programme are continuously improved.

This step-by-step process systematically evaluates feedback, analyses the scope for improvements and determines the appropriate level of escalation. By following this approach, organisations ensure that their cybersecurity exercises and portfolios remain effective and aligned with strategic objectives, and are continuously improved.

6.3 Deliverables check: moving forward phase

At this stage of the process, all main deliverables should be finalised and we are ready to start taking action in line with the findings and recommendations included in the AAR.

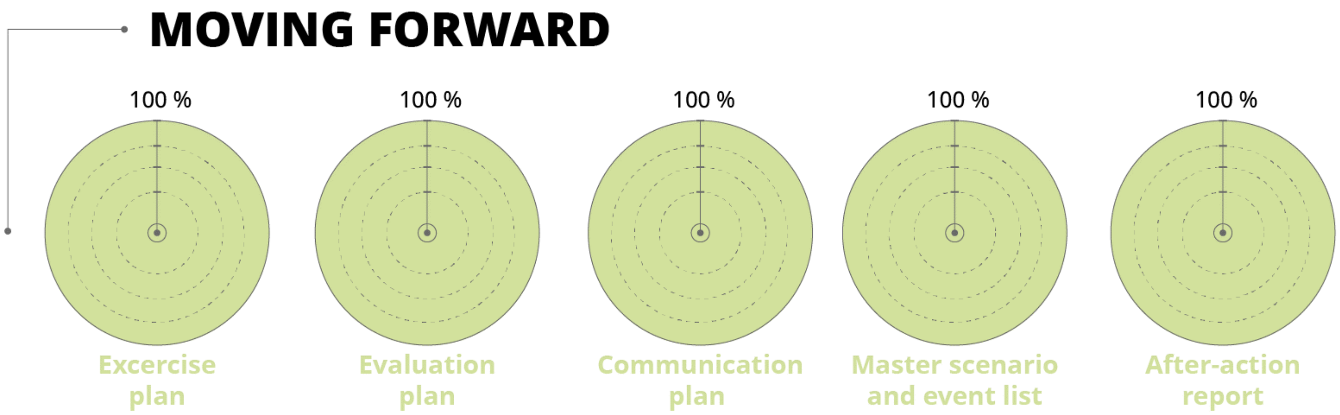


Figure 15 - Deliverable status at the end of the Moving Forward phase

Conclusions

The ENISA Cybersecurity Exercise Methodology represents a significant step forward in empowering organisations across Europe to build up and strengthen their cybersecurity resilience through systematic, well-structured exercises. By providing a comprehensive framework that guides planners from initial concept through to actionable improvements, this methodology transforms the complex task of exercise organisation into a manageable, repeatable process.

Throughout this document, we have outlined a clear pathway: from understanding why an exercise matters, through careful design and preparation, to effective execution and meaningful evaluation. Each phase builds upon the previous one, creating a cohesive approach that ensures that exercises deliver tangible value; that is, they are not just one-time events, but catalysts for lasting organisational improvement.

The journey continues

This publication marks a beginning, not an end point. The cybersecurity landscape evolves continuously, and so must our approaches to preparedness. We recognise that the true strength of this methodology lies not just in the framework presented here, but in the collective wisdom and practical experience of the cybersecurity exercise community across Europe and beyond.

We invite you – whether you are an experienced exercise planner or organising your first event – to contribute to the evolution of this methodology. Share your lessons learnt, your innovative approaches, your challenges overcome. Help us populate the support toolkit with real-world examples, practical tools and proven materials that will benefit the entire community.

Embracing innovation while preserving excellence

As we look to the future, we acknowledge that emerging technologies, particularly AI, will play an increasingly important role in exercise planning and execution. AI-powered tools promise to automate routine tasks, accelerate scenario development, enhance data analysis and streamline administrative processes. These innovations will undoubtedly make exercise planning more efficient and accessible to organisations of all sizes.

However, we remain firmly convinced that the human element – the expertise, judgement, creativity and experience of skilled planners – will always be central to delivering truly effective cybersecurity exercises. Technology can enhance our capabilities, but it cannot replace the nuanced understanding of organisational culture, the ability to adapt to unexpected developments or the wisdom to interpret results within their proper context. The most valuable exercises will always be those that combine technological efficiency with human insight, ensuring that every activity meets the highest standards of quality and relevance.

‘In cybersecurity, preparedness is not achieved through perfection, but through the continuous commitment to learn, adapt and improve.’

ANNEX A: Glossary

After-Action Report (AAR): A comprehensive document that captures exercise outcomes, findings, lessons identified, and recommendations for improvement.

Artifact: digital or physical evidence collected during an exercise for analysis and evaluation purposes.

Blue team: defensive security team responsible for protecting systems and responding to simulated attacks during an exercise.

Briefing: a structured session in which participants receive essential information about the exercise before its execution.

Capability: a measurable skill, process or resource that enables an organisation to achieve specific cybersecurity objectives.

Capability target: the desired level of performance or maturity for a specific capability being tested during an exercise.

Cold Wash: A feedback session some days / weeks after the exercise, by when participants had the time to reflect and process with some distance the experience during the exercise.

Communication plan: a structured document outlining how information will be shared with stakeholders throughout the exercise life cycle.

Compliance: adherence to relevant laws, regulations, standards and internal policies related to cybersecurity.

Core capability: a fundamental skill or process directly addressing the playing teams' actions and responses during an exercise.

Cyber range: a controlled virtual environment that simulates IT infrastructure for conducting technical cybersecurity exercises.

Debriefing: a structured discussion held after exercise execution to gather immediate feedback and observations from participants.

Discussion-based exercise: an exercise type focused on strategic discussions, decision-making and policy evaluation without operational deployment.

Drill: a focused exercise designed to test specific procedures or skills in response to particular scenarios.

Enabling capability: supporting processes, policies or tools that underpin core team operations during an exercise.

European Cybersecurity Skills Framework: a standardised framework defining 12 professional role profiles in cybersecurity across the EU.

Evaluation criteria: standards and benchmarks used to measure exercise performance and achievement of objectives.

Evaluation plan: a comprehensive document detailing how the exercise will be assessed, including methods, tools and success criteria.

Event: the highest level of scenario structure, representing major campaign themes or attack patterns spanning significant portions of an exercise.

Exercise control team: the group responsible for managing exercise execution, delivering injects and maintaining scenario integrity.

Exercise plan: a comprehensive blueprint outlining all aspects of the exercise, including objectives, scope, logistics and timeline.

Facilitator: an individual who guides exercise flow, delivers scenario elements and manages participant engagement without leading outcomes.

Finding: an identified gap, weakness, strength or observation discovered during exercise evaluation.

Hotwash: an immediate, informal debriefing session conducted directly after exercise execution to capture initial reactions.

Incident: a specific security breach or attack occurring within an event, with defined start and end times.

Indicator: an observable metric or measure used to evaluate performance against specific capability targets.

Inject: an individual piece of information, prompt or simulated action delivered to players at a specific moment to advance the scenario.

Kirkpatrick model: a four-level evaluation framework measuring reaction, learning, behaviour and results.

Lessons identified: key insights, strengths, weaknesses and improvement opportunities discovered through exercise evaluation.

Lessons learned: a change in personal or organisational behaviour that results from implementing an identified lesson to improve future performance by integrating new knowledge into practice.

Master scenario event list: a detailed timeline documenting all events, incidents and injects that drive exercise execution.

Metric: a quantitative or qualitative measure used to evaluate performance indicators.

Objective: a specific, measurable goal that defines what the exercise aims to achieve.

Observer: an individual who monitors and documents participant activities during an exercise without intervening.

Operation-based exercise: an exercise type that tests operational procedures and technical capabilities through hands-on simulation.

Planner: an individual responsible for designing, organising and managing the exercise throughout its life cycle.

Playbook: a detailed framework that outlines organisation-specific procedures for handling computer security events and incidents. It includes predefined courses of action that provide guidance on detecting, analysing and responding to potential cybersecurity threats.

Player: an individual actively participating in the exercise by responding to scenario elements as they would in reality.

Players' guide: a reference document providing participants with essential exercise information including roles, rules and logistics.

Red team: security team that simulates adversary actions by conducting controlled attacks during an exercise.

Scenario: the narrative framework that defines the simulated situation, including threat actors, timeline and sequence of events.

Scope: the defined boundaries of an exercise, including systems, participants, threat scenarios and time frames to be tested.

SMART objectives: objectives that are specific, measurable, achievable, relevant and time bound.

Stakeholder: any individual, team or organisation with interest in or influence over the exercise.

State of the world: background context describing relevant events and conditions leading up to the exercise scenario.

Storyline: the narrative sequence detailing what will happen during the exercise execution.

Tabletop exercise: a discussion-based exercise in which participants analyse and respond to simulated scenarios through collaborative dialogue.

Threat actor: the simulated adversary or attacker represented in the exercise scenario.

Threat intelligence: information about potential or current cyber threats used to inform scenario development and organisational defence.

Timeline: the schedule of activities and milestones throughout the exercise planning and execution life cycle.

Traffic light protocol: a standardised system for classifying information sensitivity (clear, green, amber, red) to control distribution.

ANNEX B: Key deliverables

Exercise Plan

The exercise plan outlines the details of the cybersecurity exercise, serving as a blueprint for its execution. The exercise plan ensures that all participants understand the exercise's purpose, expected outcomes and operational procedures, creating a cohesive strategy for success. It includes:

- **Practical details** – the execution date and related timelines, and the difficulty level;
- **Logistics and resources** – details on locations, required equipment and budget allocation;
- **Purpose and objectives** – clearly defined and measurable purpose and objectives;
- **Project plan** – a description of phases and milestones;
- **Roles and responsibilities** – identification of participants, facilitators and evaluators, along with their specific roles;
- **Scope and scenario** – the extent of the exercise, including systems, processes and personnel involved.

Evaluation Plan

The exercise evaluation plan includes all the necessary information and practical insights for planners to proceed with the evaluation of an exercise. It includes:

- **Participant roles and responsibilities** – including those of the evaluators, the people evaluated, recipients of the reports and the evaluation team;
- **Capability targets** – for a large or operation-based exercise, the capability targets to be tested during the exercise;
- **Exercise evaluation tools and methodology** – including for data collection, analysis and assessment, and reporting;
- **Evaluation timeline** – including a visual timeline covering before, during and after the exercise, and a dissemination plan.

Communications Plan

Effective communication with internal and external stakeholders is crucial for the success of cybersecurity exercises. It ensures that all parties are informed, engaged and aligned with the exercise objectives. The communication plan includes practical chronological steps for maintaining robust communication throughout planning, preparation, execution and post-exercise activities. It emphasises reaching the right stakeholders using their preferred channels and securing buy-in for continuous improvement. The table below presents the details of the communication plan.

Master Scenario Event List

The MSEL outlines the sequence of events and injects that drive the exercise, ensuring a structured and realistic simulation of cyber incidents. The MSEL can vary significantly depending on the exercise type, with tailored events and injects to suit discussion-based or operation-based exercises. It includes:

- **Events** – a list of the events planned during the exercise;
- **Incidents** – a list and practical details of all incidents related to the events planned during the exercise;
- **Injects** – individual pieces of information, prompts or simulated actions delivered to players at a specific moment to advance the scenario.

After-Action Report

The AAR documents the outcomes of the exercise. The AAR ensures that the exercise's insights are captured, leading to continuous improvement and refinement of the organisation's cybersecurity preparedness. It includes:

- **Findings and observations** – analysis of participant performance;
- **Lessons identified** – key takeaways to enhance future exercises;
- **Recommendations** – actionable suggestions for improvement;
- **Performance metrics** – evaluation of objectives met, supported by data.

ANNEX C: From objectives to capabilities

C.1 Objective themes

Further to the information included in the document on defining objectives, here is a table of objective themes to serve as inspiration for defining specific objectives.

Objective categories	Definition	Objective themes
Strategic	High-level objectives that align with the organisation's overall strategy and long-term vision	**Enhanced cybersecurity posture** – organisation's overall security measures and resilience.
		Compliance and regulatory adherence – organisation's compliance with all relevant legal and regulatory requirements.
		Risk management – management of cybersecurity risks to protect organisational assets.
Operational	Specific tasks and activities that need to be performed during the exercise	**Incident response** – organisation's ability to detect, respond to and recover from cybersecurity incidents.
		Situational awareness – ability of an organisation to accurately perceive, understand and respond to cyber threats and incidents in real time.
		Technical support and analysis – Expertise of an organisation to identify, troubleshoot and resolve security issues, and to analyse security data to prevent future incidents.
		Incident reporting – process of documenting and communicating details about security breaches or threats to ensure timely response and mitigation.
		Cooperation and information sharing – collaborative exchange of information and best practices among organisations and stakeholders.
		Communication procedures – internal and external communication during a cybersecurity event.
		Coordination and collaboration – coordination between different teams and departments during an incident.
Human factors	Human elements of cybersecurity, including awareness, training and behaviour	**Security awareness** – level of cybersecurity awareness among employees.
		Upskilling and reskilling – opportunities to upskill or reskill resources based on specific skills gaps identified during an exercise.

		Behavioural analysis – employee behaviour and adherence to security policies and procedures.
Process improvement	Identifying and improving existing processes and procedures	**Policy and procedure evaluation** – assessment of cybersecurity policies and procedures.
		Incident management process – assessment of an organisation's incident management process.
		Continuous improvement – identification of areas for continuous improvement in cybersecurity practices.
Business continuity	Ensuring that the organisation can continue operations during and after a cybersecurity incident	**Business impact analysis** – assessment of the potential impact of cybersecurity incidents on business operations.
		Disaster recovery – ability to recover from a cybersecurity incident following disaster recovery plans and procedures.
		Resilience building – organisation's resilience to withstand and recover from cyber incidents.
Compliance and legal	Ensuring adherence to legal and regulatory requirements	**Regulatory compliance** – compliance with relevant laws, regulations and standards.
		Data protection – effectiveness of data protection measures and compliance with data privacy regulations.
		Audit readiness – level of preparation for passing cybersecurity audits and assessments.

C.2 Capabilities

For more complex exercises, objectives are not enough to capture and evaluate the specific activities expected from the different teams participating in the exercise.

Capabilities serve as the critical bridge between high-level organisational objectives and the concrete actions of teams and individuals. While an objective defines what the entire organisation aims to achieve (e.g. enhance incident response time), a capability breaks this down into measurable actions for specific teams or individuals. One single objective can be tested through multiple capabilities, each assigned to different teams that must carry out their specific responsibilities during the exercise.

There are two types of capabilities, as follows.

- **Core capabilities.** These directly address the participants and focus on evaluating their actions, reactions and knowledge during the exercise. They assess how effectively participants respond to a scenario.
- **Enabling capabilities.** These focus on testing the underlying processes, policies and tools that support the core teams. They ensure that the foundational elements of the response are robust.

To facilitate precise evaluation, each capability can be linked to maturity targets that can be assessed through the exercise.

SAMPLE MATURITY TARGETS

1. **Existence:** This level examines whether a process or behaviour is present and operational.
2. **Implementation:** This level assesses the efficiency of a process or behaviour, based on criteria like speed, quality, and quantity.

Finally, to measure these targets, indicators are used. These are specific, observable metrics that guide the evaluation team on what to capture during the exercise to verify the achievement of a capability. Indicators provide the necessary link between a capability and the evaluation tools used to measure its success.

The figure below presents a summary of the journey from objectives to capabilities, indicators and metrics.

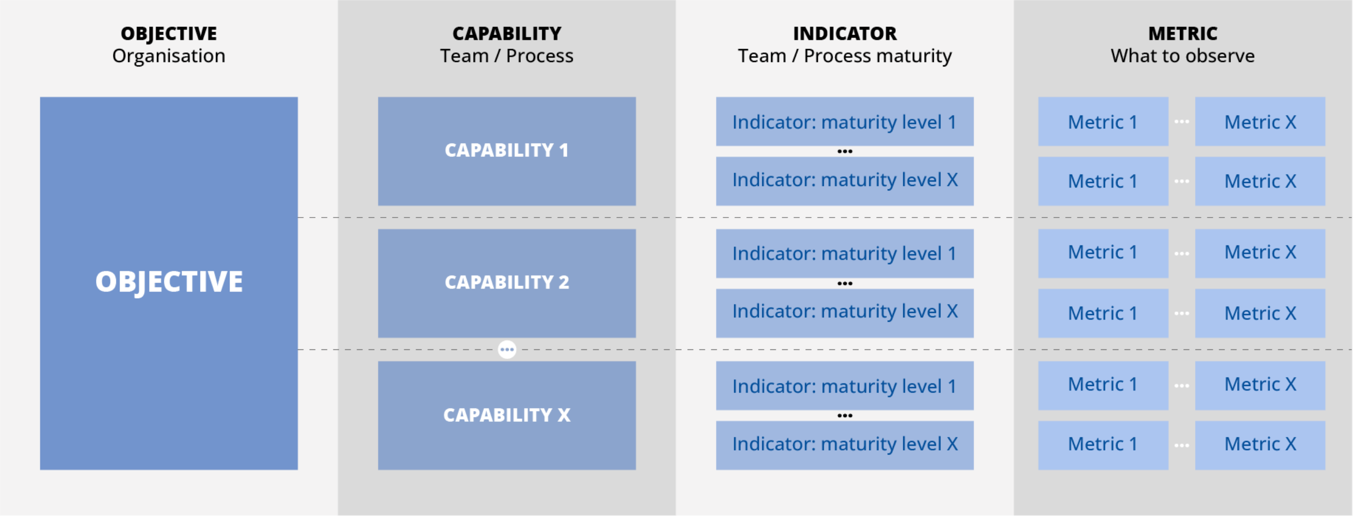


Figure 16 – From objectives to capabilities, indicators and metrics

ANNEX D: ECSF roles in the scope of exercises

The table below presents ECSF roles mapping with various exercise activities carried out by different participants of an exercise. For each exercise team, the mission is presented, the different ECSF roles that could fit on the team are mapped, and responsibilities are specified depending on a planner or player role.

Cybersecurity incident response team

Team Mission	ECSF Profiles	Profile responsibilities	
		Linked to Planner Role	Linked to Player Role
Identify and analyse threats. Coordinate containment and mitigation actions. Conduct forensic investigations.	Chief information security officer	• Define and communicate the exercise's vision, strategy, policies and procedures. • Ensure that the exercise is aligned with the organisation's overall risk management plan.	• Manage the organisation's response to the simulated cyber incident. • Assure information exchange with external authorities and professional bodies. • Ensure that business continuity and critical functions are protected during the exercise.
	Cyber incident responder	• Contribute to preparing the exercise's scenario, ensuring realism with regard to injects and timelines. • Identify and define the response procedures to be tested.	• Analyse, evaluate and mitigate the impact of cybersecurity incidents. Identify cyber incidents' root causes and malicious actors. • In accordance with the organisation's incident response plan, restore functionality of systems and processes to an operational state, collecting evidence and documenting actions taken.
	Digital forensics investigator	• Plan for the provision/collection of simulated digital evidence. • Define how artefacts should be handled and what information should be logged.	• Conduct a simulated forensic investigation to uncover the root cause and scope of the breach. • Provide analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion.
	Cyber threat intelligence specialist	• Analyse current and emerging threats to create a realistic and relevant exercise scenario.	• Analyse simulated threat intelligence feeds to identify malicious actors, their motives and their attack methods during the exercise. • Share relevant information to contribute to situational awareness efforts.

Cybersecurity engineering team

Team Mission	ECSF profiles	Profile responsibilities	
		Linked to planner role	Linked to player role
• Plan and design security-by-design solutions. • Develop, deploy and operate cybersecurity solutions. • Assess the effectiveness of security controls, and assess criticality of cybersecurity vulnerabilities if exploited by threat actors. • Research the cybersecurity domain and incorporate results in cybersecurity solutions.	Cybersecurity architect	• Design a scenario that tests the resilience of the organisation's existing security architecture. • Evaluate the effectiveness of architectural cybersecurity defences during the exercise.	• Apply security controls as part of the response effort.
	Cybersecurity implementer	• Prepare and deploy the required cybersecurity solutions in the exercise environment. • Configure the tools needed for the exercise scenario. • Operate, monitor and troubleshoot cybersecurity solutions during the simulated incident.	• Apply security controls as part of the response effort.
	Penetration tester	• Design the technical aspects of the scenario, including potential red team and blue team roles.	• Act as a 'red team' member, conducting a simulated attack against the target systems. • Act as a 'blue team' member, defending against the attack
	Cybersecurity researcher	• Conduct fundamental research on emerging threats, attack vectors and technologies to include in the exercise design. • Ensure the inclusion of innovative attack methods in the scenario to test the organisation's readiness for future threats.	• Analyse simulated data and new threat intelligence during the exercise to adapt defensive strategies in real time. • Report on novel attack techniques discovered during the response.

Cybersecurity capacity building team

Team Mission	ECSF profiles	Profile responsibilities	
		Linked to planner role	Linked to player role
• Improve cybersecurity knowledge, skills and competences of humans.	Cybersecurity educator	• Develop and deliver pre-exercise training sessions to ensure that participants have the necessary skills. • Create educational materials that support the exercise's learning objectives. • Identify and document learning gaps to inform future training needs.	• Not applicable

Legal team

Team Mission	ECSF profiles	Profile responsibilities	
		Linked to planner role	Linked to player role
• Advise on data protection laws and regulations. • Handle legal documentation and reporting. • Manage communication with regulatory bodies.	Cyber legal, policy and compliance officer	• Identify and incorporate relevant legal and regulatory requirements (e.g. GDPR, NIS2) into the exercise scenario and evaluation plan.	• Report simulated incidents in line with legal and regulatory obligations. • Ensure that compliance policies are followed during the response, recommending remediation strategies/solutions to ensure compliance.

Risk management team

Team Mission	ECSF profiles	Profile responsibilities	
		Linked to planner role	Linked to player role
• **Identify potential risks and vulnerabilities.** • **Develop risk mitigation strategies.** • **Monitor risk levels throughout the exercise.**	**Cybersecurity auditor**	• Design the evaluation and audit plan for the exercise. • Ensure that the exercise tests the organisation's compliance with internal and external standards. • Collect evidence of the response process and identify non-compliance or procedural weaknesses during the simulated incident.	• Not applicable
	Cybersecurity risk manager	• Make sure that the exercise's objectives and scope include relevant risks to the organisation.	• Make risk-based decisions during the response.

Other relevant profiles to include in cybersecurity exercises are presented in the table below.

Team	Team Mission	Profiles	Profile responsibilities
Executive management	• Approve the exercise plan and objectives. • Ensure alignment with organisational goals. • Participate in decision-making during critical points of the exercise.	**Board member** – provides governance and oversight for the organisation's cybersecurity policies and initiatives.	Ensures that cybersecurity risks are adequately managed and mitigated. Supports the development and implementation of cybersecurity strategies. Monitors compliance with cybersecurity regulations and standards.
		Chief Executive / Information / Technology Officer – oversees the overall strategic direction and operational management of the organisation's IT and cybersecurity functions.	Defines and implements the organisation's IT and cybersecurity strategies. Ensures alignment with business objectives and regulatory requirements. Promotes a culture of cybersecurity awareness and resilience across the organisation.
IT team	• Monitor and maintain system integrity. • Detect and respond to technical incidents. • Implement recovery processes.	**IT manager** – manages the IT infrastructure and operations to ensure the availability, integrity and security of digital systems and services.	Oversees the implementation of cybersecurity measures within the IT department. Coordinates with other departments to ensure that cybersecurity policies are adhered to. Manages IT staff and resources to support cybersecurity initiatives.
		System administrator – maintains and supports the organisation's IT systems and networks to ensure their secure and efficient operation.	Implements and monitors security controls on IT systems. Performs regular security assessments and updates. Responds to and mitigates security incidents.
		Network engineer – designs, implements and manages secure network infrastructure to support the organisation's operations.	Ensures the security and resilience of network systems. Monitors network traffic for suspicious activities. Implements network security protocols and measures.
Legal team	• Advise on data protection laws and regulations. • Handle legal documentation and reporting. • Manage communication with regulatory bodies.	**General counsel** – provides legal advice and support on cybersecurity-related matters to ensure compliance with laws and regulations.	Advises on legal implications of cybersecurity policies and incidents. Ensures that the organisation's cybersecurity practices comply with relevant laws and regulations. Represents the organisation in legal proceedings related to cybersecurity.
		Data protection officer – ensures the organisation's	

		compliance with data protection laws and regulations.	Monitors and advises on data protection practices. Conducts data protection impact assessments. Coordinates with other departments to ensure personal data are handled securely.
		Legal advisor – provides specialised legal advice on cybersecurity and data protection issues.	Supports the development and implementation of cybersecurity policies. Advises on legal risks and compliance requirements. Assists in the resolution of cybersecurity-related legal issues.
Communication team	• Develop communication strategies. • Handle media inquiries and public relations. • Communicate with stakeholders and customers.	**Communications director** – manages the organisation's internal and external communications related to cybersecurity.	Develops and implements communication strategies for cybersecurity awareness. Coordinates communication during cybersecurity incidents. Ensures clear and effective communication of cybersecurity policies and procedures.
		Public relations specialist – manages the organisation's public image and communication during cybersecurity incidents.	Develops and executes public relations strategies for cybersecurity incidents. Communicates with media and stakeholders during incidents. Promotes the organisation's cybersecurity initiatives and achievements.
		Internal communications coordinator – facilitates internal communication about and awareness of cybersecurity policies and practices.	Ensures that employees are informed about cybersecurity policies and procedures. Coordinates internal communication during cybersecurity incidents. Promotes cybersecurity awareness and training programmes.
Human resources team	• Organise training sessions for participants. • Ensure employee awareness and readiness. • Manage internal communications related to the exercise.	**HR manager** – manages the organisation's human resources functions with a focus on cybersecurity-related roles and responsibilities.	Develops and implements HR policies that support cybersecurity initiatives. Coordinates recruitment and training for cybersecurity roles. Ensures compliance with cybersecurity-related human resource regulations.
		Training coordinator – develops and manages cybersecurity training programmes for employees.	Identifies training needs related to cybersecurity. Develops and delivers training programmes. Evaluates the effectiveness of training programmes and updates them as needed.
		Employee relations specialist – manages employee relations with a focus on cybersecurity awareness and compliance.	Promotes a culture of cybersecurity awareness among employees. Addresses employee concerns related to cybersecurity policies. Ensures compliance with cybersecurity-related human resource policies.
External stakeholders			
Partners	• Provide support and resources. • Share threat intelligence and best practices. • Participate in joint response actions.	**Threat intelligence analyst** – analyses and monitors cybersecurity threats to provide actionable intelligence.	Collects and analyses threat intelligence data. Identifies and assesses potential cybersecurity threats. Provides recommendations to mitigate identified threats.
		Partner liaison – manages relationships with external partners to support the	Coordinates with external partners on cybersecurity matters. Ensures that partners comply with the organisation's

		organisation’s cybersecurity initiatives.	cybersecurity policies. Facilitates information exchange and collaboration with external partners.
		Response coordinator – coordinates the organisation’s response to cybersecurity incidents.	Develops and implements incident response plans. Coordinates response efforts during cybersecurity incidents. Ensures effective communication and collaboration during incidents.
Third-party vendors	• Provide cybersecurity tools and solutions. • Assist with threat detection and analysis. • Support recovery and remediation efforts.	**Vendor manager** – manages relationships with third-party vendors to ensure their compliance with cybersecurity policies.	Evaluates and selects vendors based on cybersecurity criteria. Monitors vendor compliance with cybersecurity policies. Coordinates with vendors on cybersecurity matters.
		Cybersecurity consultant – provides expert advice and support on cybersecurity matters.	Advises on the development and implementation of cybersecurity policies. Conducts cybersecurity assessments and audits. Provides recommendations to improve cybersecurity posture.
		Recovery specialist – manages the organisation’s recovery efforts following cybersecurity incidents.	Develops and implements recovery plans. Coordinates recovery efforts following incidents. Ensures the restoration of affected systems and services.

TP-01-25-028-EN-N

ABOUT ENISA

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