TLP - Clear

**Exercise Plan**

Template for a cybersecurity exercise plan

The Exercise Plan (ExPlan) is built throughout the Initiation and the Preparation phases of a cybersecurity exercise planning

february 2026

Table of Contents

1. Exercise Practical Details 2

2. Logistics and resources 3

3. Exercise Purpose and Objectives 4

4. Project Plan 6

5. Stakeholder, Roles & Responsibilities 8

6. Scope and Scenario Overview 10

7. Communication Plan 12

8. Dissemination Plan 14

# Exercise Practical Details

|  |  |
| --- | --- |
| *Exercise dates* | What are the dates planned for the exercise? |
| *Exercise timeline* | What is the timeline of the exercise, including the pre-exercise, during the exercise and post-exercise activities? |
| *Exercise type* | What is the exercise type chosen? |
| *Exercise setup* | What is the exercise setup (online, on premise, etc)? |
| *Exercise owner* | Who is the owner planner of the exercise? |
| *Exercise Classification Level* | Ex. UNCLASSIFIED, TLP:WHITE, TLP:GREEN, TLP:AMBER |
| *Exercise Complexity/Difficulty Level* | * Beginner * Intermediate * Advanced |
| *Estimated Duration* | In (hours/days for each phase) |

# Logistics and resources

|  |  |
| --- | --- |
| *Required non-human resources* | * Meeting rooms: * Technical setups: * Communication tools: |
| *Participation accommodation* | * Travel or special arrangement: * Workstation: * VPN access: |
| *Budget Allocation* | What is the foreseen budget? |
| *Cyber Security and Data protection Requirements & Measures* | What are the cyber security and data protections requirements & measures in place to protect the lifecycle of the activity?   * "Potential Risks to Real Operations" * "Safety Protocols and Kill-Switch Procedures" * "Data Protection and Privacy Measures" * "Legal/Compliance Considerations" * "Insurance/Liability Coverage" |

# Exercise Purpose and Objectives

|  |  |
| --- | --- |
| *Purpose* | What is the overall purpose or mission of the exercise? |
| Why are you organising the exercise (*max 3*)?   1. **WHY 1**: 2. **WHY 2**: 3. **WHY 3:** |
| *Objectives* | What are the specific objectives of this exercise (*max 5*)?   1. **Objective 1**: 2. **Objective 2**: 3. **Objective 3**: 4. **Objective 4**: 5. **Objective 5**: |

# Project Plan

|  |  |
| --- | --- |
| *Project high-level phases timeline* | **Initiation:**  **Design:**  **Preparation:**  **Execution:**  **Reporting:**  **Moving forward:** |
| *Schedule & Milestones* | **Consider:**   * "Dependencies and Prerequisites" (what must be completed before each phase) * "Critical Path Items" * "Go/No-Go Decision Points" * "Resource Allocation per Phase" |

# Stakeholder, Roles & Responsibilities

While a cybersecurity exercise typically involves several types of participants, including evaluators, those being evaluated, and recipients, this section will focus exclusively on the active participants, referred to as the players. The roles and responsibilities of the other participants will be thoroughly detailed in the Evaluation Plan.

|  |  |
| --- | --- |
| *Target entities* |  |
| *Planner* | Planner Name: |
| Function/responsibilities: |
| Related ECSF profile: |

|  |  |
| --- | --- |
| *Target entities* |  |
| *Players* | Player Name: |
| Function/responsibilities: |
| Related ECSF profile: |

|  |  |
| --- | --- |
| *Target entities* |  |
| *Observer* | Observer Name: |
| Function/responsibilities: |
| Related ECSF profile: |

# Scope and Scenario Overview

|  |  |  |
| --- | --- | --- |
| *Scope* | What is the scope of the exercise?   * Which specific systems will be included in the exercise? * What types of data will be involved in the exercise? * Will the exercise be conducted at a single location or multiple locations? |  |
| *Scenario overview* | Description of scenario, including the main threat actor, the main events, and the storyline: |  |
| Timeline:   * Background information: * State of the world: * Summary of incidents and other remarkable events: * Execution plot per day: |  |

# Communication Plan

For each item below, provide a description and an owner. The communication plan is dedicated to all three phases of an exercise (before, during and after an exercise) but does not include the dissemination of the results.

|  |  |
| --- | --- |
| *Communication channels* | * Emails: * Phone: * Instant messaging: * Video conferencing: * In-person meetings: |
| *Communication protocols* | Incident reporting: |
| Status updates: |
| Coordination meetings: |
| Escalation procedures: |
| Documentation: |
| *Key Contacts* |  |
| *Communication schedule* | Provide an estimated time of communication per activity and channel. |

# Dissemination Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Audience** | **Audience Type** | **Dissemination tool** | **Confidentiality/Classification Level** | **Communication schedule** |
| *All* | Combination |  |  |  |
| *Participating Audience* | Exercise Players   * Cross-Functional teams * Technical teams * Departmental teams * Remote teams |  |  |  |
|  |  |  |
| Exercise Planners |  |  |  |
|  |  |  |
|  |  |  |
| Exercise observers |  |  |  |
| *Non-Participating Audience* | Rest of the organisation |  |  |  |
| Press |  |  |  |
| General public |  |  |  |
| Management board |  |  |  |

|  |
| --- |
| About ENISA |
| The European Union Agency for Cybersecurity, ENISA, is the Union’s agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union’s infrastructure, and, ultimately, to keep Europe’s society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu. |
| **ENISA**  European Union Agency for Cybersecurity  Athens Office  Agamemnonos 14  Chalandri 15231, Attiki, Greece  Brussels Office  Rue de la Loi 107  1049 Brussels, Belgium |