TLP-CLEAR

**Cybersecurity Exercise Request**

Template to request the organisation of a cybersecurity exercise

february 2026

Table of Contents

1. Organisation 2

2. Timeframe 4

3. Exercise characteristics 5

4. Purpose & Objectives 6

5. Expected outcomes 8

6. Resource, Stakeholders & Budget 10

# Organisation

|  |  |  |
| --- | --- | --- |
| *Name of the agency / entity / organisation* |  |  |
| *In which category does your organisation fall under?* | * EU CSIRT Network Member * EU CYCLONE Member * EU Member States Public Authority * EUIBA * NIS Cooperation Group Member * Private Organisation * Public Organisation * Other: |  |
| *Organisation's Sector(s) /Industry* | **List of Applicable Sectors as per NIS2 as per the directive**  [EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex](https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng) |  |
| *Exercise Planner Owner* | **Name**:  **Contact details**: |  |
| *Primary Point of Contact (POC) for Technical Issues* | **Name**:  **Contact details**: |  |
| *Other Exercise Planners involved* | **Name**:  **Contact details**: |  |
| **Name**:  **Contact details**: |  |
| **Name**:  **Contact details**: |  |
| *Maturity* | Have you and/or your organisation planned, co-planned, observed a cyber exercise in the past? Specify your past role(s)   * Planner * Observer * Co-Planner * None of the above   **Comment**: |  |
| Have you and/or your organisation participated in an ENISA organised cyber exercise in the past? In case of previous participation, please specify the exercise.   * Yes * No   **Comment**: |  |

# Timeframe

|  |  |  |
| --- | --- | --- |
| *Proposed date of the exercise* |  |  |
| *Proposed duration of the exercise* | * 4 hours / half day * 8 hours / one day * 2 days * Other: …. |  |
| *Proposed timeframe until execution of the exercise* | * 3 months * 6 months * 12 months * 18 months * Other: …. |  |

# Exercise characteristics

|  |  |  |
| --- | --- | --- |
| *Priority linked to NIS2* | Specify any exercise registered in your application that is of high priority and will improve the security posture of EU critical infrastructure elements as specified by the NIS2 directive and how (if applicable). Please select the choice consistent with your description:   * Link with NIS2 and defined high priority. * Link with NIS2 but no determined priority. * No link with NIS2 but with high priority. * No link with NIS2 and no determined priority.   **Comment**: |  |
| *Exercise type* | Please select the type of exercise that you are interested (select all that apply):   * Type 1 – Discussion-based Exercises * Type 2 – Operation-based Exercises   **Comment**: |  |
| *Exercise Complexity Level* | * Beginner * Intermediate * Advanced |  |
| *Geographic Scope* | * Sectorial * National * Regional * Eu-wide * International |  |
| *Exercise Package Type* |  |  |
| *Exercise Short name* |  |  |
| *Exercise Brief Description* |  |  |

# Purpose & Objectives

|  |  |  |
| --- | --- | --- |
| *Exercise mission* |  |  |
| *Exercise purpose (WHY)*  *Max 3* | **Why 1:** |  |
| **Why 2:** |  |
| **Why 3:** |  |
| *Exercise Objectives*  *Max 5* | **Objective 1:** |  |
| **Objective 2:** |  |
| **Objective 3:** |  |
| **Objective 4:** |  |
| **Objective 5:** |  |

# Expected outcomes

|  |  |  |
| --- | --- | --- |
| *Impact* | How many professionals do you anticipate enhancing their cybersecurity skills and capabilities through the envisioned exercise?   * Less than 20 professionals * 20-50 professionals * 51 – 100 professionals * 101 – 250 professionals * Over 250 professionals   **Comment**: |  |
| Based on the latest ENISA Foresight report, which cybersecurity threats do you believe this exercise will most effectively enhance your organisation’s preparedness against?   * Supply Chain Compromise of Software Dependencies * Skill Shortage * Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems * Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem * Rise of Digital Surveillance Authoritarianism / Loss of Privacy * Cross-border ICT Service Providers as a Single Point of Failure * Advanced Disinformation / Influence Operations (IO) Campaigns * Rise of Advanced Hybrid Threats * Abuse of AI * Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure |  |
| *Expected outcome* | In an ideal scenario, what outcome do you expect from this exercise for each of the categories below:   * **Compliance of policies, procedures, and processes:** * **Cybersecurity awareness and skills:** * **Cooperation, coordination, and communication:** * **Situation awareness and incident response:** * **Incident reporting & communication:** |  |

# Resource, Stakeholders & Budget

|  |  |  |
| --- | --- | --- |
| *Exercise resource required* | Expected number of planners:   * High (over 50 participants) * Medium (11-49 participants) * Low (less than 10 participants)   **Comment**: |  |
| *Stakeholders involved* | Please tick the box of every type of stakeholder involved.   * Executive Leadership: * IT and Security Teams: * Risk Management: * Legal and Compliance: * ommunication and Public Relations: * External Partners:   **Comment**: |  |
| *Budget consideration* |  |  |