Challenge 04

Prove the Protections

Exercise	Operation Electro Magnetic Panic
First run	17 October 2025, Madrid, Spain
Published by	303 Overwatch A.S.B.L, R.C.S. Luxembourg F13274
Licence	CC BY-SA 4.0. Free to run, adapt and share.

This brief is contributed as open, non-commercial work in support of exercise and workforce development obligations under the NIS2 Directive. It is guidance, not legal advice.

303 Overwatch A.S.B.L, 10 rue Willy Goergen, L-1636 Luxembourg
www.303overwatch.org • workforce.development@303overwatch.org

Contents

Challenge 4, Prove the Protections

Scoring Model

Condition	Points
First team to submit	+10 bonus
Submission within Hour 1	+10 base
Submission within Hour 2-3	+5 base
Submission after Hour 3	0 base
Each missing or unsubstantiated AICM control implementation	-5 each
Maximum penalty	-15 points

> **Important:** Unlike Challenge 3, which focused on mapping, this challenge requires **operational evidence** showing that selected controls are truly implemented and functioning.

1. Objective

Teams must **demonstrate and evidence the implementation** of at least three AICM control objectives previously mapped in Challenge 3. This is about proving that governance and security controls are not just documented but **real and observable** in the system.

Example control areas include:

- Governance/Oversight
- Model Governance
- Data Minimization
- Monitoring & Auditing
- Access Control
- Encryption & Cryptography
- Incident Response / Recovery

The goal is to connect declared security posture with **tangible operational artifacts**.

2. Required Capabilities

A. Control Implementation

- Select at least **three control objectives** from your AICM mapping table in Challenge 3.
- Show how these controls are **operationally enforced** in your running deployment.
  - Example: If you mapped *Access Control*, show Basic Auth or other identity enforcement in action.
  - If you mapped *Data Minimization*, show sanitized logging or restricted data flow.

B. Evidence Capture

- Collect clear, relevant evidence for each control. Acceptable forms include:
  - Log excerpts showing security-relevant events.
  - Configuration snippets demonstrating enforcement of policies.
  - Screenshots of access control, monitoring dashboards, or key security settings.
  - Command outputs verifying control operation.

C. Residual Risk & Trade-Offs

- For each control, provide a short **narrative (2-4 sentences)** explaining:
  - The residual risk that remains after the control is implemented.
  - Any trade-offs (e.g., complexity, performance, cost, usability) made in applying the control.

3. What Will Be Provided to Teams

- A **Google Docs folder**

4. Submission Deliverable

When the team has gathered evidence:

Create a password-protected Word document named:

team-<TEAM_NUMBER>-prove-the-protections.docx

2. Inside the document, include:
    - List of the three (or more) AICM control objectives being evidenced.
    - For each control:
        - The **AICM domain and control objective**.
        - A **short description** of the control.
        - **Evidence artifacts** (log snippet, config, screenshot, etc.).
        - A **2-4 sentence residual risk and trade-off narrative**.
    - Optional: any additional links or references (e.g., to specific code commits).
3. Set a **password** for the file.
4. Upload it to the **Google Docs challenge folder**.
5. Send the password securely to the mentor (e.g., Slack DM).

5. Mentor Evaluation Process

Once the file is received, mentors will:

- Check that at least three **distinct AICM control objectives** are evidenced.
- Verify the relevance and authenticity of the submitted logs/configuration/screenshots.
- Read the residual risk narratives for:
    - Accuracy in describing realistic remaining risk.
    - Awareness of trade-offs made in implementation.
- Apply a **5-point deduction** for each missing or weakly substantiated control.

6. Minimal Compliance Checklist (Mentor View)

- At least three distinct AICM control objectives are evidenced.
- Evidence is relevant and tied to the mapped control.
- Evidence clearly demonstrates operational enforcement (not just planning).
- Each control has a residual risk narrative (2-4 sentences).
- Narratives demonstrate realistic understanding of trade-offs.

7. Additional Guidance for Teams

- Think “audit-ready.” Your evidence should be something a reviewer could validate independently.
- Avoid generic screenshots or boilerplate text; show your specific configuration or log data.
- Make sure timestamps, command outputs, or configuration context are clear.
- Residual risk narratives should be **specific**, not generic (e.g., “a motivated adversary could still…” rather than “there is always risk”).
- Trade-offs may include reduced performance, operational complexity, or additional maintenance burden.

8. Summary of Submission Flow

1. Select at least three AICM controls from your Challenge 3 mapping.
2. Collect operational evidence for each control.
3. Write residual risk and trade-off narratives.
4. Prepare a password-protected Word document with evidence.
5. Upload to the Google Docs challenge folder.
6. Send the password securely to the mentor.
7. Mentor will inspect and score.

9. Example Evidence Structure (For Reference)

Domain	Control Objective	Evidence Artifact
Access Control	Enforce authentication for all endpoints	Screenshot of Basic Auth prompt, curl -I 401 re
Data Minimization	Prevent disclosure of unnecessary metadata	Log snippet showing filename suppression in c
Logging & Monitoring	Detect anomalous activity	Container logs, failed login attempts logged wi