Challenge 03

Map the Mind: Apply AICM

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 3, Map the Mind: Apply AICM

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 incomplete domain/control mapping	-5 each
Maximum penalty	-25 points

> **Important:** This challenge evaluates teams' ability to think beyond implementation and **connect security controls to governance and assurance frameworks**.

1. Objective

Teams must apply the AICM (AI Control Mapping Framework) to their deployed RAG system from previous challenges. The goal is to:

- Identify **at least five relevant AICM domains**, and
- Map **at least one control objective per domain** to a concrete implementation artifact in their system (for example, a configuration, control, or process they have actually implemented).
- Provide a **short risk summary** for each mapped control, demonstrating an understanding of how it mitigates relevant threats.

This challenge assesses security alignment, traceability, and the ability to reason about risk in operational deployments.

2. Required Capabilities

A. AICM Domain Identification

- Select a minimum of five domains from AICM that apply to the deployed solution. Examples may include:
  - **Data Management**
  - **Access Control**
  - **Cryptography**
  - **Logging and Monitoring**
  - **Model Governance**
  - **Infrastructure Security**
  - **Incident Response and Recovery**

(Teams may select other relevant domains if justified.)

B. Control Objective Mapping

- For each selected domain, identify **one control objective** and map it to **an actual implementation artifact** in your system.
  - Example: Data Management → Encrypted stores configured (Qdrant at-rest encryption + TLS)
  - Example: Access Control → Basic Auth with password protection on all endpoints

C. Risk Summary

- Provide a **2-4 sentence risk summary** for each mapped control that:
  - Describes what risk or threat the control mitigates, and
  - Explains why it matters in the context of your system.

3. What Will Be Provided to Teams

- A **Google Docs folder**

4. Submission Deliverable

When the team has completed the AICM mapping:

Create a password-protected Word document named:

team-<TEAM_NUMBER>-aicm-mapping.docx

2. Include in the document:
    - Deployment URL (for reference only; no mentor testing of endpoints this round)
    - AICM mapping table in CSV or Markdown format with the following columns:
        - Domain
        - Control Objective
        - Implementation Artifact
        - Risk Summary (2-4 sentences)
    - Optional: references or links to relevant sections of configuration or code if needed to clarify the mapping.
3. Set a **password** for the file.
4. Submit 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:

- Review the AICM mapping table.
- Confirm at least five **distinct** domains are used.
- Check that each control objective has a clear, concrete implementation artifact.
- Read each risk summary to ensure it demonstrates:

- Understanding of the threat/risk context.
- Reasonable alignment between control and risk.

5-point deductions will be applied for each missing or incomplete domain/control mapping.

6. Minimal Compliance Checklist (Mentor View)

- At least five unique AICM domains mapped.
- One control objective per domain.
- Each mapping linked to a real implementation artifact.
- Each mapping includes a risk summary (2-4 sentences).
- Mapping table is clear and structured.

7. Additional Guidance for Teams

- Focus on **traceability**, not volume. One well-articulated control per domain is sufficient.
- Your mapping should make it clear **how** your implementation satisfies or supports the control.
- Write the risk summaries as if presenting to a stakeholder-concise, clear, and context aware.
- Choose domains that are most relevant to your deployment; avoid superficial mappings.
- It is acceptable (and encouraged) to reference decisions made in Challenge 1 and Challenge 2.

8. Summary of Submission Flow

1. Identify at least five relevant AICM domains.
2. Map one control objective per domain to an actual artifact in your deployment.
3. Write 2-4 sentence risk summaries for each.
4. Prepare a password-protected Word document with your table.
5. Upload it to the Google Docs challenge folder.
6. Send the password securely to the mentor.
7. Mentor will inspect and score.

9. Example Mapping Table (for Reference)

Domain	Control Objective	Implementation Artifact
Data Management	Ensure protection of sensitive data at rest	Encrypted Qdrant volume using
Access Control	Enforce strong authentication on all endpoints	Basic Auth with secure passwor
Cryptography	Protect communications using secure protocols	TLS 1.3 enforced on all app and
Logging and Monitoring	Detect anomalous behavior through logging	Container-level logging and prox
Incident Response	Provide mechanisms for rapid containment and recovery	Container restart policy + encryp