

TRANSPORT AUTHORITY 1 – EXECUTIVE COMMITTEE BRIEFING

SUBJECT: *Escalating Cyber-Threat Landscape*

DATE: 23 February 2026

CLASSIFICATION: **Highly Confidential – Executive**

1. Overview

This briefing provides an update on the current cyber-risk environment affecting the Authority's operational, administrative, and customer-facing systems. Recent assessments indicate an elevated threat posture requiring strategic decisions on risk mitigation.

2. Key Issues

2.1 Funding Request: Project SHIELD

- The Chief Information Security Officer (CISO) submitted a request for an additional **€10M** to advance *Project SHIELD*, the Authority's proposed next-generation intrusion detection and monitoring programme.
- The **Finance Committee declined the request**, citing competing capital priorities.
- During the session, the CEO stated:

"We are a transport authority, not a tech company. We must prioritize visible infrastructure."

- Impact: Deferral of Project SHIELD extends the current detection-capability gap into the next fiscal cycle.

2.2 Red Team Assessment – Signaling Network

- The internal Red Team conducted an end-to-end assessment of the Authority's **legacy signaling network**.
- Findings: The network was assessed as **"highly vulnerable to a dedicated attacker"**, primarily due to age, architectural constraints, and limited segmentation.
- Estimated mitigation cost: **€4.5M**.
- **Status:** *Unfunded*. No corrective works currently scheduled.

3. Residual Risk Considerations

- Both issues materially increase potential operational disruption exposure.
- Maintaining the current posture without investment may elevate regulatory scrutiny and insurance-related risks.

4. Recommended Executive Actions

1. Re-evaluate the *Project SHIELD* funding decision during the mid-year budget review.
2. Commission an accelerated options analysis for signaling-network risk reduction.
3. Direct the CIO and CISO to prepare consolidated risk-impact projections for Q2.