

12–18 OCTOBER 2026

Define Resilience Brief

ISSUE 08 examines OT protection, the implementation of NIS2 measures in Microsoft 365, and eligibility for the STEP and Defense funding program.

01

CYBERSECURITY • OT/ICS • BUSINESS CONTINUITY

Could someone take control of your refrigeration or production systems over the internet?

The National Cyber Security Authority (NCSA) has identified more than 300 internet-exposed systems in Greece, mainly commercial refrigeration controllers.

FACT:

On 14 October, the NCSA urged critical infrastructure operators to disconnect control systems from the public internet. It identified more than 300 exposed systems in Greece, mainly commercial refrigeration controllers. Its recommendations include allowing remote access only through a VPN with multi-factor authentication (MFA), changing default credentials, installing security updates, and replacing equipment that is no longer supported.

WHY IT MATTERS:

An exposed controller could turn a cyber incident into loss of control over refrigeration or production, product spoilage, and operational disruption. This is immediate protective guidance; it does not announce a new statutory deadline.

WHO IS AFFECTED

Businesses using refrigeration controllers or other OT/ICS systems, especially in food, supermarkets, cold storage, manufacturing, and energy facilities.

SOURCE: [NCSA-Exposed industrial controllers](#)

ACTION — OT SECURITY CHECKS:

- OT/ICS equipment, internet connectivity, and operational owners have been recorded.
- Direct public access has been removed; remote maintenance is performed through a VPN and MFA.
- Default credentials have been changed and available security updates are being applied.
- Unsupported equipment has been identified and a secure replacement is planned.
- The business continuity plan covers loss of refrigeration or production and safe recovery.

MANAGEMENT QUESTION:

- Do we know which OT systems are exposed, and how quickly can we limit the damage and keep operations running?

02

NIS2 • MICROSOFT 365 • GOVERNANCE

Microsoft 365 and NIS2: a license does not prove compliance

The right Microsoft 365 subscription provides security tools, but does not prove that controls have been enabled and are working.

FACT:

On 16 October, the NCSA introduced a free online tool to help organizations compare Microsoft 365 plans against their cybersecurity needs and the requirements of Joint Ministerial Decision (JMD) 1689/2025 and the NIS2 Directive. The announcement clarifies that the right license provides technical tools, but does not, by itself, ensure compliance.

WHY IT MATTERS:

The gap often lies between the features included in a license, the settings actually applied, and the evidence that controls are working. The announcement does not establish a new obligation or deadline.

WHO IS AFFECTED

Organizations within the scope of NIS2 and businesses that rely on Microsoft 365 for email, identities, devices, and data.

SOURCE: NCSA-[16 October 2026 announcement](#) | [Free tool](#)

ACTION — MICROSOFT 365 CHECKS:

- Applicable requirements are mapped to the licenses purchased and the users assigned to them.
- Critical capabilities, including MFA, anti-malware protection, and audit logging, are enabled and correctly configured.
- Evidence of control implementation and operation is retained, with clear ownership and periodic review.
- Gaps, costs, and remediation priorities are documented; the license selection is confirmed with the relevant licensing partner.

MANAGEMENT QUESTION:

- Can we demonstrate that the security controls available in our Microsoft 365 environment are enabled, implemented, and reviewed?

03**FUNDING • STEP • CYBERSECURITY TRAINING****50% funding for STEP and DEFENCE training, subject to eligibility criteria**

The STEP and DEFENCE programme has a €20 million budget and covers 50% of eligible training costs, subject to specific participation criteria.

FACT:

The call, published on 13 October, is for existing businesses that meet the conditions, including: 100 unique employees in 2025 (distinct tax IDs recorded in ERGANI, not annual work units); an eligible or related activity code (KAD); and a strategic focus on STEP or DEFENCE. The budget is €20 million, with 50% support for eligible costs. Applications are open from 2 November to 31 December 2026 and are assessed in order of priority.

WHY IT MATTERS:

Eligibility depends on more than company size or the subject of the training: the training must relate to the company's activity, and all conditions must be met. Statutorily mandatory training is not eligible for funding.

WHO IS AFFECTED

Businesses with at least 100 unique employees in the most recently completed year and documented relevance to STEP strategic technologies or the DEFENCE sectors.

SOURCE: [OPSKE call](#) | [Full call \(PDF\)](#)

ACTION — CHECK BEFORE APPLYING:

- The 100-employee threshold is confirmed through ERGANI, and the KAD and relevance to STEP or DEFENCE are checked.
- The training plan addresses business needs and documents the maintenance or increase of overall training expenditure.
- Eligible and ineligible costs are calculated, including statutory mandatory training, which is not funded.
- Supporting documents are prepared in time for online applications from 2 November, and the order of priority is monitored.

MANAGEMENT QUESTION:

- Can we document that we meet every criterion, and do we have a well-developed training plan before applications open?

[READ ALL ISSUES ↗](#)

We help organizations manage regulatory, digital, and operational risks through oversight.



Managing risk. Enabling growth.