Managing risk. Enabling growth.

26 OCTOBER – 1 NOVEMBER 2026

Define Resilience Brief

This week highlights three operational priorities for Greek businesses: agree what outsourced IT providers will do when a critical vulnerability is found, resolve any outstanding annual financial statement filings with G.E.MI., and assess eligibility for the new STEP and defence training grant.

01

CYBERSECURITY • NIS2 • THIRD-PARTY RISK

Outsourcing IT does not transfer cyber resilience accountability

You rely on an external IT provider. Have you agreed what it must do in the first 24 hours after a critical vulnerability is identified?

THE FACT:

On 26 October, the Hellenic National Cyber Security Authority published the findings of the sixth Cyber Greece conference, held on 21 October. Hellenic National Defence General Staff officers said Greece faces more than 1,000 serious cyberattacks a day. The discussion also highlighted how AI can accelerate attacks and increase pressure on critical infrastructure. No new regulatory obligation was announced.

WHY IT MATTERS:

Outsourcing IT to an MSP, cloud provider or other third party does not transfer management accountability. Responsibilities, response times and evidence must be clear for vulnerability monitoring and remediation, privileged access, backups and incident escalation. After a critical patch, reviewing logs can help establish whether a compromise occurred beforehand.

WHO IS AFFECTED

Businesses using outsourced IT, managed service providers, cloud or hosting providers, and external network administrators. NIS2 entities and organisations in health, energy, water, transport, industry and the public sector face particular exposure.

SOURCE: Hellenic National Cyber Security Authority, 26 Oct 2026 ↗

ACTION - CHECK NOW WITH YOUR IT PROVIDERS:

- Name owners and response times for vulnerability monitoring, assessment and remediation.
- Protect third-party accounts with MFA, least privilege and regular access reviews.
- Test backups and require the provider to evidence a successful restoration.
- After critical patches or a suspected incident, review logs for signs of earlier compromise.
- Make sure contracts and incident plans define escalation and support for required notifications.

MANAGEMENT QUESTION:

- If a critical vulnerability were disclosed today, could we show who does what in the first 24 hours?

02

CORPORATE COMPLIANCE • GOVERNANCE • G.E.MI.

G.E.MI.: ten-day compliance window after the new warning

G.E.MI.: companies with outstanding annual accounts will receive a new notice and a ten-day window to comply.

THE FACT:

On 30 October, the G.E.MI. Service clarified that the messages sent about unpublished financial statements were informational warnings. The filing and publication deadline remained 31 October 2026. Companies that still have an outstanding filing will receive a new warning giving them ten days to complete the obligation.

WHY IT MATTERS:

The 31 October deadline has passed; the notice does not create an automatic extension or remove the filing obligation. The ten-day period starts when the new warning reaches the company. Monitoring the corporate email account and G.E.MI. inbox is essential: failure to resolve the filing may lead to suspension of registry entries and complicate corporate transactions or due diligence.

WHO IS AFFECTED

Companies and other entities required to publish annual financial statements in G.E.MI., together with their boards, finance teams, accountants and corporate advisers.

SOURCE: G.E.MI. – One-Stop Services, 30 Oct 2026 ↗

ACTION - CHECK YOUR G.E.MI. FILING NOW:

- Confirm whether the 2025 financial statements have been filed and published.
- Monitor the company email account and G.E.MI. inbox for the new warning.
- Record when the notice arrives and calculate the ten-day period from that date.
- Agree with your accountant or legal adviser which documents or corrections are outstanding and who will file them.

MANAGEMENT QUESTION:

- Who is monitoring the new G.E.MI. notice, and can they resolve the filing within the deadline it sets?

03

FUNDING • STEP • WORKFORCE SKILLS

Applications open for STEP and defence training

Applications open today at 15:00 for STEP and defence training. Is your business eligible?

THE FACT:

Applications to the in-company training scheme open on 2 November 2026 at 15:00 and close on 31 December at 15:00. The €20 million scheme funds 50% of eligible plans, with project budgets of €150,000–€1.2 million. Applicants must meet the 100-employee threshold, counted as unique individuals in the last full calendar year, qualify under the eligible activity code rules and show a clear link to STEP or defence and security.

WHY IT MATTERS:

The grant supports defined in-company training in eligible sectors, not general off-the-shelf courses. Applicants need a documented skills assessment, a clear link to their production or technology activities, an eligible activity code and a budget that meets the call requirements.

WHO IS AFFECTED

Existing businesses with at least 100 employees and an eligible activity or a documented connection to STEP strategic technologies or the defence and security sectors.

SOURCE: EFEPAE – Competitiveness Programme, 2 Nov 2026 ↗

ACTION - CHECK BEFORE APPLYING FOR STEP FUNDING:

- Check that the business meets the employee threshold and the call's eligibility criteria.
- Verify the eligible activity code and document the link to a STEP or defence and security priority.
- Prepare a training plan with clear needs, employee groups, objectives and measurable outcomes.
- Check eligible costs, budget and conditions before submitting through OPSKE.

MANAGEMENT QUESTION:

- Can we show that the training plan directly supports an eligible technology or activity and a specific business need?

Βοηθάμε οργανισμούς να διαχειρίζονται
κανονιστικούς, ψηφιακούς και λειτουργικούς κινδύνους
με εποπτεία.

Managing risk. Enabling growth.