MBB
MALTA BUSINESS BUREAU

POLICY BRIEF
FEBRUARY 2026

Cybersecurity Act

mbb.org.mt

and the EU in managing cybersecurity threats - similar to what existing standardisation bodies are doing.

The Cybersecurity Act will be applicable immediately after approval by the European Parliament and the Council of the EU. The accompanying the Network and Information Security Directive (NIS2) amendments will also be presented for approval. Once adopted, Member States will have one year to implement the Directive into national law and communicate the relevant texts to the Commission.

Key Provisions of the Revision of the Cybersecurity Act (CSA)

The CSA is aimed at:

- ✓ ICT Producers and Vendors: Organisations manufacturing or providing digital products and services will be subject to more extensive, stringent, and uniform certification requirements throughout the European Union.
- ✓ Users of Critical Technology: Businesses (such as those in healthcare, finance, telecommunications etc...) that leverage high-stakes technologies will be required to synchronise their internal risk management frameworks with established European cybersecurity benchmarks.
- ✓ Essential Service Providers: Entities operating in vital industries—such as energy, finance, and telecommunications—will be responsible for auditing and managing their level of reliance on any suppliers flagged as "high risk."

The revision focuses on harmonising the EU's fragmented cybersecurity landscape by aligning the CSA with other major legislations like NIS2 and the Cyber Resilience Act (CRA). A central objective is to foster a "once-only" reporting culture, where cybersecurity certification schemes under the renewed framework serve as evidence of compliance with NIS2 obligations. While this streamlines supervision and incident reporting, it presents a transitional challenge for companies that have recently finalised their NIS2 compliance strategies. Ultimately, the revision aims to ensure that ICT products, services, and processes are verified as trustworthy across the entire supply chain, bolstered by increased investment in R&D and European technology.

ENISA's Mandate – A Greater Role for ENISA

Under the new proposal, the ENISA transitions into a more central, steering role. Moving beyond simple cooperation, it is proposed that ENISA will now be empowered to engage directly in standardisation activities, including drafting technical specifications and assisting the Commission in assessing harmonised standards. Its operational scope is also expanding to include:

- Certification Steering: Taking the lead on schemes for cloud services, 5G, and Managed Security Services (MSS).
- Operational Support: Providing situational awareness, capacity building, and assistance in implementing cyber rules across Member States.
- Active Defence: Collaborating with Europol to address ransomware through a dedicated Helpdesk for victimized entities.
- Vulnerability Management: Maintaining a centralised EU vulnerability database and establishing methodologies for coordinated disclosure.

European Cybersecurity Certification Framework

The European Cybersecurity Certification Framework (ECCF) upgrades existing certification schemes to cover the full ICT chain. While certification generally remains voluntary, it may be mandated by specific EU rules when dealing with critical infrastructure (such as technologies in energy grids, hospitals etc...). A notable governance shift includes the replacement of the Stakeholder Cybersecurity Certification Group (SCCG) with a new European Cybersecurity Certification Assembly. Key operational changes include:

- ENISA now faces a statutory 12-month deadline to deliver candidate certification schemes.
- For certifications at the "high" assurance level, assessment activities must be performed within the European Economic Area (EEA) to mitigate risks from external interference.
- The framework will introduce schemes to certify an entity’s "cyber posture," where entities can demonstrate they are managing cyber risks effectively.

Security of ICT Supply Chains

This section introduces a robust—and potentially controversial—framework for identifying and blacklisting high-risk suppliers. If a supplier is designated as "high-risk" following a sector-specific analysis, public authorities and critical operators may be barred from purchasing their equipment.

The legislative proposal seeks to create a framework for reliable ICT supply chains. Under this system, either the European Commission or a minimum of three Member States may request that the NIS Cooperation Group perform a coordinated security risk assessment at the Union level, which must be completed within a six-month window.

Exclusion Criteria for High-Risk Vendors

If a supplier is designated as "high-risk" following this assessment, they will face specific prohibitions: they will be barred from contributing to the development of EU standards under Regulation 1025, rendered ineligible for EU cybersecurity certificates, and excluded from both public procurement tenders and the receipt of EU funding.

Enforcement and Mitigation

To enforce these measures, the Commission will adopt implementing acts to officially blacklist certain suppliers and mandate a specific phase-out period for the removal of their components. Additionally, a separate implementing act will be introduced to establish required mitigation measures.

Third-Country Mapping and Exemptions

The Commission is also tasked with mapping suppliers that are either established in or controlled by third countries identified as posing security risks. During this process, the provider will be granted the right to be heard. Furthermore, a provision in the current text exists for entities to request a formal exemption, even if they are associated with a country deemed to be a risk.

Institutional Friction

It is noted that the high degree of discretion the Commission has reserved for itself in these matters may cause friction with Member States, particularly because the NIS2 Cooperation Group is given only a restricted role within this specific section of the legislation.

Sector-Specific Implementation

In accordance with Articles 110 and 111, the Commission will publish a list of high-risk vendors specifically concerning mobile electronic communication networks, with a requirement that relevant components be phased out within 36 months—an initiative that builds upon the foundations of the 5G security toolbox. Furthermore, Recital 133 highlights other critical sectors where cybersecurity risks are prevalent, including autonomous vehicles, surveillance technology, the electricity sector, and water management systems.

A Company Perspective:

The revision of the Cybersecurity Act will fundamentally reshape how businesses operating within or providing digital services to the EU manage their operations. These changes are categorised into five primary pillars.

1. Governance and Risk Management

Organisations will be expected to demonstrate a sophisticated level of cybersecurity maturity. This requires moving beyond securing individual products and instead embedding robust policies, oversight mechanisms, and control structures that prove effective risk management across the entire organisation.

2. ICT Products, Services, Processes, and Certification

The broadened certification framework now encompasses cloud computing, 5G, managed security services, and general organisational "cyber posture." This expansion results in:

- Increased regulatory oversight for technology vendors.
- Higher financial and time investments required to bring products to market in sensitive industries.
- Enhanced security guarantees for businesses that rely on third-party digital tools and infrastructure.

3. Supply Chain and Technological Dependencies

The introduction of tools to identify and ban high-risk suppliers will directly alter global supply chain strategies. Key consequences include:

- Continuous monitoring of strategic and geopolitical risks associated with vendors.
- The potential need to "rip and replace" existing hardware or software, leading to significant financial and operational strain.
- A comprehensive re-evaluation of interconnected systems, such as energy equipment, solar inverters, and data centres.
- Increased costs for SMEs, who may become more dependent on a smaller pool of certified suppliers.
- A "chilling effect," where customers pre-emptively avoid certain vendors who might be labelled high-risk, even before official measures are taken.

4. Operations and Incident Response

With ENISA taking a more prominent role and the introduction of a centralised reporting platform, companies will face more rigorous notification duties. This will directly increase the workload and required capacity of Security Operations Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs).

5. Regulatory Compliance and Administrative Burden

While the long-term goal is a unified regulatory landscape, the transition will be demanding. Organisations will need to dedicate substantial resources to technical, legal, and documentary updates to ensure they align with the new framework.

The Maltese Perspective

In terms of the "Rip and Replace" costs for High-Risk Vendors (HRVs) as mentioned above, it is important to note that Malta's core 5G and fibre networks are already largely "clean," relying primarily on trusted European vendors. Therefore, the risk of Maltese operators needing to physically replace antenna masts or core routers is low compared to other EU states.

The proposal with its annexes can be accessed here.

Disclaimer: This is a policy brief to create awareness about the legislative proposal and for information purposes. It is not an official position of the Malta Business Bureau.

For questions or more detailed information please contact Christine Cassar – Senior Projects Executive on infobrussels@mbb.org.mt

The Malta Business Bureau is the EU advisory organisation of;

THE MALTA CHAMBER

MHRA MALTA HOTELS & RESTAURANTS ASSOCIATION

and a partner of the Enterprise Europe Network;

enterprise europe network

Business Support on Your Doorstep