European Commission

#DSM

Digital Single Market

EU CYBERSECURITY ACT

ENISA AND CYBERSECURITY CERTIFICATION FRAMEWORK

In order to scale up the EU's response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single Market, the EU Cybersecurity Act:

- Strengthens ENISA, the **European Union Agency for Cybersecurity** to improve the coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies;
- Establishes an **EU cybersecurity certification framework** that will allow the emergence of tailored certification schemes for specific categories of ICT products, processes and services. Companies will be able to certify their products, processes and services only once and obtain certificates that are valid across the EU.

The EU Agency for Cybersecurity (ENISA)

The EU Cybersecurity Act gives the existing European Agency for Network and Information Security (ENISA) more tasks and resources in order to assist EU Member States in dealing with cyber-attacks. This will be done with:

- ☑ **A strong mandate**
- ☑ **A permanent status**
- ☑ **Adequate resources**

ENISA resources	Now	Future
Staff	84 people	125 people
Budget	€11 million	€23 million
	gradual increase: starting with +5 million 1st year and fully achieved 4 years after entry into force.	

ENISA will improve the EU's preparedness to react by organising regular pan-European cybersecurity exercises and by contributing to better information sharing between EU Member States through the network of Computer Security Incident Response Teams (CSIRTs). It will help EU Member States to implement the Directive on the Security of Network and Information Systems (NIS Directive) which clarifies reporting obligations of national authorities in case of serious incidents. ENISA will also support the establishment and maintenance of the EU cybersecurity certification framework.

Main new tasks

Policy development and implementation: to strengthen support to the Commission and Member States in the development, implementation and review of general cybersecurity policy and in key strategic sectors identified by the NIS directive e.g. energy, transport and finance.

Operational cooperation: to contribute to cooperation in the network of Computer Security Incident Response Teams (CSIRTs) at EU level and provide assistance on request to Member States to handle incidents.

Knowledge and information: to provide analyses and advice and to raise awareness, to become the one-stop shop (InfoHub) for cybersecurity information from the EU Institutions and bodies.

Capacity building: to reinforce support to Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents.

Market-related tasks within the **Cybersecurity Certification Framework** facilitate the preparation of the candidate European cybersecurity certification schemes, with the expert assistance and in close cooperation with national certification authorities. Schemes should be adopted by the Commission. ENISA will also support policy development in information communications technolgy (ICT) standardisation.

An EU framework for cybersecurity certification

What is it for?

Certification plays a critical role in increasing trust and security in products and services that are crucial for the Digital Single Market. At the moment, a number of different security certification schemes for ICT products exist in the EU. Without a common framework for EU-wide valid cybersecurity certificate schemes, there is an increasing risk of fragmentation and barriers in the single market.

How will the certification process work?

The **EU Agency for Cybersecurity, ENISA**, with the help of national experts will prepare the technical ground for the certification schemes that will then be adopted by the European Commission through implementing acts. The EU-wide certification framework creates a comprehensive set of rules, technical requirements, standards and procedures to agree each scheme. Each scheme will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. smart cards. This certificate will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified cybersecurity requirements. The resulting certificate will be recognised in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

Is the use of the certification framework compulsory?

No. The use of certification schemes will be voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific cybersecurity need. The European Commission will assess the possible need for mandatory certification for certain categories of products and services.

The lifecycle of a European Cybersecurity Certification Scheme