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 ENISA, the EU Agency for Cybersecurity, 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 cybersecurity preparedness and resilience, contributing to better information sharing between EU Member States through the network of Computer Security Incident Response Teams (CSIRTs) and organising regular pan-European cybersecurity exercises and trainings. 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 cybersecurity incidents. ENISA will also have a central role in establishing and supporting the implementation of the EU cybersecurity certification framework.

Main ENISA tasks under the new mandate

Policy development and implementation: to provide support to the European Commission and EU 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 strengthen the existing preventive operational capabilities, support operational cooperation as secretariat of the network of Computer Security Incident Response Teams (CSIRTs) at EU level and provide assistance on request to EU 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 EU 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** prepare candidate European cybersecurity certification schemes, with the assistance of experts and close cooperation with national certification authorities. Schemes would be adopted by the European Commission together with EU Member States. ENISA will also support policy development in information communications technololgy (ICT) standardisation.

Updated 26 June 2019

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.

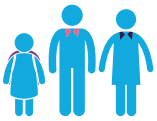
Is the use of the certification framework compulsory?

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. However, the European Commission will assess the possible need for mandatory certification for certain categories of products and services.

How citizens and businesses will benefit from the certification framework

For an SME

Take the example of an SME that develops and sells ICT applications to larger companies that require certain assurances that the applications are appropriately secure and that they have been developed following best practices when it comes to secure coding. Using a European Cybersecurity Certificate, that SME can demonstrate both the security of its products as well as its secure development practices and hence meeting the requirements of its clients not only in one EU Member State but also across the whole of the EU.



For citizens

Take the example of a citizen who is considering purchasing a Smart TV but is also aware about the cybersecurity risks involved when connecting similar smart objects to the Internet.

The European citizens can consult ENISA's European Cybersecurity Certification website. They will be able to find a model that has been certified with the appropriate cybersecurity requirements but also more information including guidance from the vendor on how to setup, configure and operate the TV in a secure way and for how long the vendor commits to provide cybersecurity patches if new vulnerabilities are found.

Besides, vendors of ICT product and services will be keen to make buyers aware possibly by using a specific label linked to the certificate.