Radio Equipment Directive Cybersecurity Services

RED Article 3.3 Cybersecurity

- Article 3.3(d) applies to devices related to network protection.
- Article 3.3(e) applies to equipment that processes personal data, traffic data or location data.
- Article 3.3(f) applies to radio equipment that enables the holder or user to transfer money, monetary value, or virtual currency.

Scope of the new regulation

The new regulation shall apply to any radio equipment that can communicate itself over the internet, whether directly or via other equipment. Radio equipment that may expose sensitive personal data is also in scope. For example:

- Mobile phones, tablets and laptops
- Wireless toys and children's safety equipment, such as baby monitors
- Wearable devices, such as smartwatches and fitness trackers

Out of scope devices

- A device that only connects to the internet via a cable connection, without radio equipment (e.g. wifi, ble), is out of the scope for this regulation.
- Shall not apply to radio equipment to which any of the following Union legislation also applies:
  a. Regulation (EU) 2018/1139
  b. Regulation (EU) 2019/2144
  c. Directive (EU) 2019/520

UL Solutions

The European Commission's (EC's) Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for radio equipment, setting essential requirements for safety and health, electromagnetic compatibility (EMC), and radio spectrum efficiency.

The directive includes Article 3.3 as a placeholder to address device requirements related to radio-specific issues ranging from common interfaces to cybersecurity.

On Jan. 12, 2022, the Official Journal of the European Union published delegated regulation 2022/30/EU, enforcing compliance requirements to RED Article 3.3(d), (e) and (f). The regulation increases cybersecurity, personal data privacy and fraud protection for applicable wireless devices available in the European Union (EU) market. It took effect on Feb. 1, 2022, and will become mandatory on Aug. 1, 2025, giving device manufacturers a 42-month transition period.

UL Solutions offers Internet of Things (IoT) security services designed to support you in every step of your journey toward RED compliance, from initial strategy and development through formal compliance and product launch.

Safety. Science. Transformation.™

UL Solutions RED cybersecurity services

The RED Delegated Act (RED DA) will impact any manufacturer producing radio equipment to be sold in the EU market. Manufacturers will be responsible for cybersecurity throughout the entire life cycle of the device. While the harmonized standards are not yet published, you can begin preparing for compliance now.

UL Solutions advisory services can help you progress toward RED DA compliance by highlighting gaps and providing you with education and guidance to reach your objectives. We can work together to increase your cybersecurity resiliency in alignment with the cybersecurity regulation landscape.

UL Solutions can support you regardless of your current development stage. For early-stage projects, we can help you apply security by design (SbD) and embed security in your governance and processes. To this end, our trainings and workshops led by our security experts can help equip your team with the knowledge to successfully implement your products.

For projects in a later development stage, we can assist you with a gap analysis or full compliance assessment to EN 303 645 and IEC 62443-4-2, which will help you increase the security posture of your products. These two standards have requirements that overlap with the requirements expected to be in the harmonized standards for RED DA, and compliance with these standards will greatly support your readiness for the RED.

RED DA and EU regulatory landscape workshop

The workshop covers the EU cybersecurity regulatory background and landscape. First, we will provide an overview of the EU cybersecurity regulatory background, which will set the stage for a deeper understanding of the current state of affairs. Next, we will dive into the specifics of the RED Delegated Act for Article 3.3 (d)(e)(f) and its importance in enhancing the security and privacy of connected devices, along with the future impacts of the Cyber Security Resilience Act. We will also explore the role of ETSI EN 303 645 in providing a common cybersecurity baseline for IoT devices to be a step toward compliance.

The workshop lasts approximately four to six hours and can be delivered remote or on-site.

Journey toward RED compliance

Basic – Level 1: Initiation

This service is designed for manufacturers starting their journey into the RED DA and are looking for an expert to identify the major gaps toward future compliance. This is an ideal solution when cybersecurity-related documentation is not in a coherent state. The benefit for the manufacturer is that they can start from a solid foundation with the support of a RED DA expert.

This package includes a review of an ETSI EN 303 645 (aligned with the draft harmonized European standard) gap analysis as well as a report and presentation highlighting major roadblocks on the journey toward RED DA compliance.

Substantial – Level 2: Developing

This service is designed for manufacturers that have already started working on their compliance with RED DA and have prior experience with cybersecurity certifications. They already have performed a self-assessment/gap analysis and would like subject matter experts (SMEs) to evaluate their work to make sure they are going in the right direction. More solid documentation is available to be reviewed by RED DA experts that can drive the conversation in a more detailed manner.

This package includes the same services as the basic level plus a deeper documentation review, including additional IEC 62443-4-2 provisions that are aligned with the draft harmonized European standard. The report and presentation will also include a more detailed analysis and a road map that considers additional potentially applicable regulatory requirements of the Network and Information Security 2 (NIS2) Directive and the European Cyber Resilience Act (CRA).

High – Level 3: Defined

This service is designed for manufacturers that are well on track on their journey to compliance with RED DA and are looking for an expert to evaluate their work. Moreover, they are seeking deep knowledge to perform security testing of their device to evaluate the security controls implemented in alignment with the requirements.

This package includes the same services as the substantial level plus a vulnerability assessment and the relative vulnerability scanning report.

Why UL Solutions for cybersecurity?

- Independent, trusted third party
- Hardware- and software-based security evaluations
- Cybersecurity expertise
- Cybersecurity and safety
- Full life cycle solutions
- Assessment of security development practices
- Industry knowledge
- Global teams and local support

Cybersecurity foundation

- Expertise in global standards and frameworks
- Extensive knowledge of best practices
- Growing list of Internet of Things (IoT) security solutions

To learn more and contact our experts, visit UL.com/RED.

UL Solutions

UL.com/Solutions