Cybersecurity Requirements in the Radio Equipment Directive

Understand the scope, timelines and how to prepare for compliance

About the Radio Equipment Directive

The European Commission's (EC) Radio Equipment Directive (RED) 2014/53/EU establishes a regulatory framework for radio equipment, setting essential requirements for safety and health, electromagnetic compatibility (EMC) and radio spectrum efficiency. Radio equipment is defined as an electrical or electronic product that intentionally emits and/or receives radio waves for the purpose of radio communication and/or radio determination. Every Internet of things (IoT) or connected device has a common consideration that uses radio or wireless technology, so, in general, most IoT devices fall under the RED's scope.

To regulate radio products, the RED has a set of rules called essential requirements, which comprise the minimum set of requirements that a radio product needs to fulfill to demonstrate compliance with the RED. These essential requirements are set in Article 3 of the RED.

- **Article 3.1 A –** Safety and health requirements
- **Article 3.1 B –** EMC requirements for radio equipment
- **Article 3.2 –** Specific requirements for radio products and the efficient use of the radio spectrum
- **Article 3.3(d)(e)(f) –** Cybersecurity requirements

Scope of RED Article 3.3 for cybersecurity

RED Article 3.3(d)(e)(f) specifies a minimum set of cybersecurity requirements for network protection, protection of personal data and privacy, and protection from fraud of non-cash-based transactions. These requirements have been present in the directive, but as of Feb. 1, 2022, the EC has activated and enforced Article 3.3(d)(e)(f), making it mandatory with a transitional period of 42 months.

The definition of such devices per the RED includes devices that are internet-connected or devices that process data with connectivity, such as:

- 4G/LTE/5G-enabled devices
- Wi-Fi-enabled devices
- Bluetooth®-enabled devices
- Radar equipment
- Televisions and radio receivers
- GPS transceivers
- RFID device

UL Solutions

Harmonized standards and notified bodies

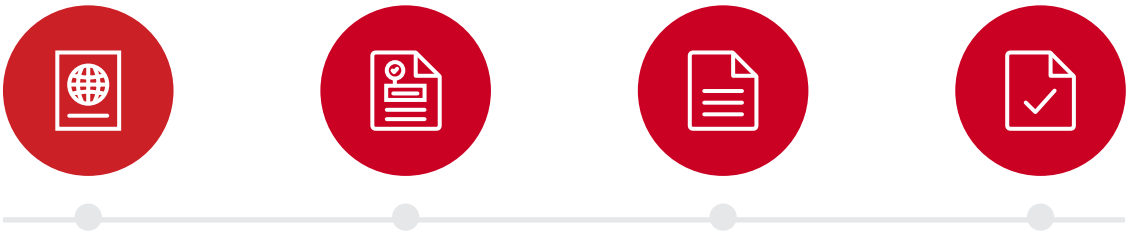
While the EU has activated essential requirements for Article 3.3(d)(e)(f), there are no agreed-upon harmonized standards yet. However, the EU has made reference to the fact that harmonized standards will be made available 13 months prior to the transition date of August 1, 2025, bringing it to June 30, 2024.

If there is no harmonized standard, Article 17 and Annex III of the Directive note that the conformity assessment procedure needs to be carried out by an EU-type examination with a Notified Body, making it mandatory.

At UL Solutions, we are a registered Notified Body currently undergoing the necessary training and acceptance for submission through the necessary accreditation bodies.

Timelines

On Feb. 1, 2022, the 42-month transitional period began. This timeline strikes a good balance between the urgent need to improve the level of cybersecurity of radio equipment on the European market and the need to allow manufacturers reasonable time to adapt their products. In the interim, however, organizations need to get ready for these dates and will need to use this transition period to get compliant and apply their readiness



January 12, 2022

Official Journal of the EU published delegated regulation 2022/30/EU, enforcing compliance requirements to RED Article 3.3(d), (e) and (f).

February 1, 2022

Official Journal of the EU activated RED Article 3.3. (d), (e) and (f), starting the 30-month transition period.

June 30, 2024

Harmonized standards are expected to be released.

August 1, 2025

Hard deadline for compliance to RED Article 3.3 (d), (e) and (f), at which point it becomes mandatory.

42-month transition period

Prepare for compliance

It is important to note that cybersecurity is based on layers and that the objective of the RED is to create a minimum requirement of compliance for the EU. However, cybersecurity is a very dynamic environment, with constantly evolving risks from zero-day vulnerabilities to policy and procedure requirements.

We propose that manufacturers need to apply “security by design” and embed security in the governance and processes of all manufacturers at the early stages of product design and development. It is important not to leave security to the final testing phases, as this could significantly impact readiness and result in missing the timelines.

Additionally, for manufacturers to remain competitive, they need to enable brand protection through security assurances and be agile to deploy products into multiple markets with a single certification or under a complete security framework addressing these concerns. UL Solutions can help manufacturers at every step.

UL Solutions

Cybersecurity capabilities

We offer a comprehensive suite of cybersecurity services to meet you right where you are in your cybersecurity journey. Our services include testing, certification and other advisory services to successfully launch connected products. These include:

- **Organizational cybersecurity governance services –** Evaluate processes, procedures and security governance principles
- **Cybersecurity evaluations, testing, compliance assessments and surveillance services –** Assessments to regional and local guidelines and standards such as ETSI EN 303 645 (EU), NIST/Global Acceptance (U.S.), TEC 31318 (India), Code of Practice for Consumer IoT Security (U.K.), National Cybersecurity Labeling Scheme (Singapore), AS4755.2 (Australia)
- **Ancillary connected services across mobile and web –** Penetration testing and vulnerability analysis
- **Compliance assessments for security and privacy for cloud computing –** Assessments such as ISO 27001 and Cloud Security Alliance's STAR Program
- **Other fit-for-purpose cybersecurity services –** Evaluations to IEC 62443 for industrial IoT, Common Criteria for government-based schemes, FIPS for cryptography in the U.S. and Canada, ISO 21434 for automotive or ANSI UL 2900, the Standard for Software Cybersecurity for Network-Connectable Products, for medical and smart buildings
- **Broad range of advisory services –** Help our customers with market enablement and certification readiness

Your comprehensive service provider

UL Solutions also offers additional services, including testing, certification and advisory, for electrical safety, EMC wireless, market access, Bluetooth qualification, Zigbee and Thread. Let us be your comprehensive service provider for connected device acceptance into markets around the world.

For more information on the RED cybersecurity requirements, visit UL.com/RED. To get started on your device security journey, visit UL.com/cybersecurity.

UL Solutions

Safety. Science. Transformation.™

CS578651
050.02.0623.EN.CYB.