RED FAQs

Our experts provide answers to frequently asked questions about the cybersecurity requirements in the Radio Equipment Directive (RED).

Update March 2024

Q: Is there any information on the recently proposed Cybersecurity Resilience Act (CRA) and its interaction with the cybersecurity requirements in the Radio Equipment Directive (RED)? Also, what is the latest information on direct versus indirect connection to the internet?

A: The scope of the CRA covers a broader array of devices, software and situations than defined in the scope of RED Article 3.3(d)(e)(f) as it addresses "products with digital elements." However, there are overlaps. The CRA has the potential to supersede and repeal RED Art.3.3(d)(e)(f).

When defining the impacts of directly vs. indirectly connected devices in terms of RED Art. 3.3(d)(e)(f):

- Article I of Article 3.3(d) of Directive 2014/53/EU shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ("internet-connected radio equipment").
- The essential requirement set out in Article 3.3(e) applies to devices that are not internet-connected in cases where the device handles personally identifiable information (PII).

Q: Many IoT devices rely on mobile companion apps. Will RED Art. 3.3 apply to sensitive data, e.g., Wi-Fi passwords stored in a mobile app?

A: Details on the technical scoping requirements for the RED are not yet published as harmonized standards. The revised date for the standardization request for harmonized standards of RED Art.3.3(d)(e)(f) has been extended from October 2023 to December 2023. Once the harmonized standards are released, additional clarity will be provided.

Q: Are generators in-scope with RED cybersecurity if they have telemetrics in them?

A: The RED applies to products classified as radio equipment in reference to typical communication equipment such as radio transmitters and wireless phones as well as a wide range of products that integrate LoRaWAN, Wi-Fi, Bluetooth®, NFC, ZigBee, Z-Wave and other wireless technologies in all kinds of consumer and professional electronic equipment.

However, the applicability of RED Art. 3.3(d)(e)(f) also depends on existing directives where the devices may be exempt when they apply to other directives such as:

- Medical devices under Regulation (EU) 2017/745 and (EU) 2017/746
- Radio equipment under Regulation (EU) 2018/1139 for civil aviation
- Radio equipment under Regulation (EU) 2019/2144 for motor vehicles
- Radio equipment under Directive (EU) 2019/520 for road toll systems

Accordingly, depending on the use case of the product, it would fall under RED Art. 3.3(d)(e)(f). If products fall under the scope of RED Art. 3.3(d)(e)(f) and are not preceded

by another directive, they could also fall into one of two categories against which we can evaluate products: EN 303 645 for consumer products or IEC 62443 for industrial products.

RED FAQs

Q: Is industrial radio equipment that talks to hubs/ gateways in or out of scope?

A: RED Art. 3.3(d)(e)(f) addresses devices connected directly or indirectly. It would, however, depend on the use case and any additional supporting applicable directives. The hub/gateway would be the focus of RED compliance in this instance, as would the connected device. Please refer to ETSI EN 303 645 and IEC 62443 (both already published) until the European Commission publishes the relevant harmonized standards.

Q: How does the RED apply to existing products in the market?

A: Products must comply with the regulations and directives in force when they're manufactured and the Declaration of Conformity (DoC) is issued, meaning existing stock of pre-RED Art. 3.3 (d)(e)(f) RED-compliant devices comply. However, it is still in manufacturers' best interests to provide secure products to the market. For detailed explanations, please refer to the European Commission's Blue Guide.

Q: Does RED Art. 3.3(d)(e)(f) require Notified Body certification, or can the vendor internally evaluate it? Also, please describe the requirement for RED devices for industrial applications.

A: RED Art. 3.3 (d)(e)(f) will align with the existing European Commission rules for compliance as described in the Blue Guide. You can secure an evaluation through a Notified Body or with a self-assessment against harmonized standards, but a Notified Body would be required in the absence of notified standards. In other words, testing will be done against the essential requirements per applicable standards to show conformance, e.g., ETSI EN 303 645 for consumer devices and IEC 62443 industrial automation and control system devices (with some additional tests required). Industrial and consumer IoT devices fall within the scope of RED Art. 3.3(d)(e)(f).

Q: Do you have a more accurate view of adopting necessary standards in the EU due to the issue between the European Telecommunications Standards Institute (ETSI) and the European Commission?

A: ETSI has published the most well-known security standard for consumer Internet of Things (IoT) devices, ETSI EN 303 645. However, ETSI has been excluded from the standardization request for RED Art. 3.3(d)(e)(f). ETSI EN 303 645 has become the baseline for the majority of IoT security evaluations globally with coverage of 80% of the specifications defined in the essential requirements of RED Art. 3.3(d)(e)(f).

The EU agrees with the content of ETSI EN 303 645; however, its scope is limited to a specific set of consumers' IoT devices and use cases. Accordingly, when published, we expect the ETSI EN 303 645 standard to heavily influence harmonized standards.

Q: Do the RED and ETSI EN 303 645 require a secure boot or full root of trust applied to all executable files?

A: ETSI EN 303 645 addresses secure boot and full root of trust, but they are not mandatory for all devices. The harmonized standards will likely take a similar approach.

RED FAQs

Q: Does UL Solutions already have a conformance assessment checklist for compliance with RED cybersecurity requirements? Will these points only affect the products released after August 2024? If yes, what about the products in the distributor's stock? Would they have to return it to suppliers?

A: The essential requirements act as a baseline or checklist of requirements against RED Art. 3.3(d)(e)(f). We collaborate with our customers to align with ETSI EN 303 645 and the UL IoT Security Rating Gold Level requirements. These requirements align with what the European Commission has communicated and will be in the final harmonized standards.

Products must comply with the regulations and directives in force upon manufacture and DoC issuance, meaning existing stock of pre-Art. 3.3(d)(e)(f) RED cyber-compliant devices will be facceptabl . Please refer to the European Commission's Blue Guide.

Q: The examples provided in the webinar are all for endpoint devices. What about access point wireless routers? Are they in scope?

A: Yes, these devices will likely be in the scope of RED Art. 3.3(d)(e)(f). According to the Commission Delegated Regulation (EU) 2022/30, Article 3.3(d) will apply to all internet- connected radio equipment, with some exceptions for products that have other regulations. Wireless routers and access points will be in the scope of RED Art. 3.3(d)(e)(f).

Q: For EMC, safety and radio testing, on-site testing is performed against harmonized standards to gain compliance and justify the DoC. Is this the same principle for Article 3.3, and if so, how can we perform testing before the harmonized standard's release?

A: Yes, it will be the same for Article 3.3. In the absence of harmonized standards, devices must meet the essential requirements. Manufacturers can refer to the ETSI EN 303 645 standards, which are expected to influence the development of the harmonized standards.

Q: Will IoT devices used in the laboratories by forensic science teams comply with RED criteria? Currently, does ETSI EN 303 645 apply to these devices? Will the RED also apply to products using IoT devices in pharmaceutical laboratories or pharma companies?

A: These IoT devices will likely be in scope for the RED if there are no other security requirements specifically designed for this product category. Currently, ETSI EN 303 645 focuses on consumer IoT devices. Per the European Commission, "Regulation (EU) 2017/745 of the European Parliament and of the Council lays down rules on medical devices, and Regulation (EU) 2017/746 of the European Parliament and of the Council lays down rules on in vitro diagnostic medical devices. Both Regulations (EU) 2017/745 and (EU) 2017/746 address certain elements of cybersecurity risks associated with the risks addressed by Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU."

RED FAQs

Q: Are medical devices within the scope of RED cybersecurity requirements? Please clarify the medical devices exclusion mentioned. Does the radio accessory to a medical device still fall under the RED?

A: No, medical devices are not within the scope of RED Art. 3.3(d)(e)(f). See: Commission Delegated Regulation (EU) 2022/30 of Oct. 29, 2021, Article 2: "By way of derogation from Article 1, the essential requirements set out in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU shall not apply to radio equipment to which either of the following Union legislation also applies:

- Regulation (EU) 2017/745 (medical device regulation);
- Regulation (EU) 2017/746 (in vitro diagnostic medical devices (IVD))"

Q: Are industrial IoT devices within the scope of the RED? Is it safe to say that industrial IoT devices designed for a fixed location are entirely out of the scope, regardless of the wireless technology employed?

A: This would depend on a review of the devices in question. Industrial IoT devices have cybersecurity posture and capabilities that, due to their intended use and end customer, exceed those of consumer IoT. However, for compliance requirements, RED Art. 3.3(d)(e)(f) may still apply. Therefore, while these devices will likely be in scope for the RED, they will also probably meet most, if not all, of the requirements. The formal publication of the harmonized standards will provide clarity. However, as IEC 62443 and ETSI EN 303 645 have been mapped to the essential requirements of RED Art. 3.3(d)(e)(f), we can help customers demonstrate compliance by performing the relevant evaluations with minor additional evaluations/testing in the absence of harmonized standards.

Q: What is the standard number that will be available? Is it in some written form now (draft, committee draft for vote (CDV), etc.)? Do UL Solutions laboratories in Taiwan and China have this test and verification capability? Are Bluetooth-equipped devices without Wi- Fi considered IoT devices? Would a home appliance be in scope if it has Bluetooth for remote control, but an app on the user's Android or iOS device?

A: We are still unaware of the standard number, as no draft version of the harmonized standard has been released yet. UL Solutions has teams in laboratories globally — including in China and Taiwan — t that will seek updated accreditation to perform to perform all validations required for compliance with RED Art. 3.3(d)(e)(f). The specifics of each device vary, but broadly speaking, Bluetooth-connected devices are in scope for the RED, putting the device you mentioned in scope.

Q: How can I assess whether my radio- equipped product falls under RED Art. 3.3?

A: The text of the RED itself lays out a good measuring stick of what types of devices are in or out of scope. For further reference, especially in terms of existing devices and how new mandates and directives such as RED Art. 3.3 will affect them, the European Commission's Blue Guide is the best reference. A UL Solutions subject matter expert can help you identify the requirements for your product.

Q: How can we prepare our devices now?

A: Until the official harmonized standards are published in Q4 2023, we have asked manufacturers to refer to ETSIEN 303 645 and IEC 62443, which are already published standards that heavily influence the development of harmonized standards.

RED FAQs

Q: If a device falls under the RED, are the new clauses (d), (e) and (f) mandatory, regardless of product function? Do older devices already on the market need to be redesigned to implement the new clauses if we want to ship after August 2024?

A: Products must comply with the regulations and directives in force upon manufacture and issuance of the DoC, meaning existing stock of pre-RED Art. 3.3(d)(e)(f) RED-compliant devices should be fine. For detailed explanations, please refer to the European Commission's Blue Guide.

Q: Does ETSI EN 303 645 apply to Bluetooth products such as headphones?

A: Yes. ETSI EN 303 645 focuses on consumer IoT devices and applies to network-connected consumer products. Bluetooth is considered a network, even when used in a point-to-point mode. While ETSI EN 303 645 attempts to be technology-agnostic, it includes two examples with Bluetooth, indicating that Bluetooth products are in scope.

Q: If you have a radio frequency (RF) product — call this Product A— that does not connect to the internet itself but communicates via RF protocol to another RF product, B, which itself connects to the internet through LAN or Wi-Fi, is Product A within the scope of the cybersecurity requirements of RED Art. 3.3(d)(e)(f)? Product A does not communicate any personal data.

A: Yes, Product A would be in scope. Article 1 of Delegated Act 2022/30 states that it "shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment." Product A communicates with the internet via Product B and would therefore be in scope.

Q: Once RED Art. 3.3(d)(e)(f) comes into force, how can we show compliance? Will laboratories like UL Solutions offer a testing service, or will it be more like a review?

A: There will be two routes to demonstrate compliance: via a Notified Body such as UL Solutions or via self-assessment. UL Solutions offers support with training, gap analysis, evaluations and testing and conformance reports, which provide capabilities to ultimately demonstrate compliance.

Q: Once the RED is in force on Aug. 1, 2024, what does that mean for products already in the market? Do they need to retroactively comply with RED 3.3? How would that work since these devices are already certified?

A: Products must comply with the regulations and directives in force upon manufacture and issuance of the DoC, meaning existing stock of pre-RED Art. 3.3(d)(e)(f)-compliant devices should be fine. For detailed explanations, please refer to the European Commission's Blue Guide.

Q: Our company makes printers that do not store information but connect to the internet. Does 3.3 apply?

A: RED Art. 3.3(d) applies to internet-connected products to ensure that products do not negatively affect the network. A connected printer would need to comply with Art. 3.3(d). Article 3.3(e) applies to radio products that process personal, traffic or location data. A printer is likely to process personal data, even if only temporarily; therefore, Article 3.3(e) would also apply.

RED FAQs

Q: Does a device fall under the new RED only if it communicates sensitive data?

A: No, RED Art. 3.3(d)(e)(f) applies to products regardless of sensitive data.

Q: Typically, IoT products use a cloud to connect. How does the security of the physical IoT and its RED application influence the cloud software and its certification?

A: We will not know the exact specifics until the harmonized standards are published. However, most existing global consumer IoT security standards focus almost exclusively on the device itself, including ETSI EN 303 645. Cloud-based auditing capabilities are separately available to execute against the target of evaluation from an audit perspective or penetration testing.

Q: We have seen the deadline of Aug. 1, 2024, but as I understand it, this affects not only new products starting production but also existing products still in production after that date. For example, suppose a new batch of a current product is produced after this date and shipped to stores. In that case, the latest batch must comply with the RED cybersecurity requirements, even if it is the same hardware and software configuration sold in September without this requirement. Is this correct?

A: Currently, UL Solutions collaborates with its customers to align with ETSI EN 303 645 and the UL IoT Security Rating Gold Level requirements. These align closely with what the European Commission has communicated will be in the final harmonized standards. Generally, products must comply with the regulations and directives in force upon manufacture and issuance of the DoC, meaning existing stock of pre-RED Art. 3.3(d)(e)(f) cyber-compliant devices should be fine. Please refer to the European Commission's Blue Guide.

Q: What do you think about the IEC 62443 standard versus the new harmonized standard that will be released?

A: RED Art. 3.3(d)(e)(f) will align with the existing European Commission rules for compliance as described in the Blue Guide. You can demonstrate compliance through a Notified Body or self-assessment against harmonized standards, but a Notified Body would be required in the absence of notified standards. In other words, testing will be done against the essential requirements or per applicable standards, such as ETSI EN 303 645 for consumer devices and IEC 62443 for industrial automation and controls systems (with some additional tests required), to show conformance. Industrial and consumer IoT devices are within the scope of RED Art. 3.3(d)(e)(f). Further clarity will likely be provided once the harmonized standards are released.

Q: Do products outside of consumer IoT devices fall under RED Art. 3.3?

A: RED Art. 3.3(d)(e)(f) applies to network-connected radio devices. This definition is broader than consumer IoT and may include industrial and commercial devices and those using short-range communications such as Wi-Fi, Bluetooth and Zigbee.

RED FAQs

Q: Why, in the mapping slide from the webinar, are the last three rows of RED Art. 3.3(d)(e)(f) and ETSI EN 303 645 shown as black? Are they not mapping with RED requirements?

A: When the harmonized standards are released, there will be requirements within them for the essential requirements; there isn't a precise one-to-one mapping between the broad categories of RED Art. 3.3(d)(e)(f) and those particular components of ETSI EN 303 645. However, additional tests can be completed in conjunction with ETSI EN 303 645 to fulfil the requirements in the absence of harmonized standards.

Q: What testing will be required to demonstrate compliance to cybersecurity under the RED or ETSI EN 303 645, and how are these tests performed?

A: For an example of the tests and methodologies used in evaluating compliance, we suggest referring to the test specifications for ETSI EN 303 645 and ETSI TS 103 701; however, we can also perform additional tests to demonstrate compliance with the essential requirements.

Q: Assuming the harmonised standards will be late, how should manufacturers demonstrate compliance to a Notified Body?

A: RED Art. 3.3 (d)(e)(f) will align with the existing European Commission rules for compliance as described in the Blue Guide. You can secure an evaluation through a Notified Body or with a self-assessment against harmonized standards, but a Notified Body would be required in the absence of notified standards. In other words, testing will be done against the essential requirements per applicable standards to show conformance, e.g., ETSI EN 303 645 for consumer devices and IEC 62443 industrial automation and control system devices (with some additional tests required). Industrial and consumer IoT devices fall within the scope of RED Art. 3.3(d)(e)(f).

Q: Can I use a third party for testing and assessment and then self-declare without a notified body?

A: You can secure an evaluation through a Notified Body or with a self-assessment against harmonized standards, but a Notified Body would be required in the absence of notified standards.

UL Solutions

Safety. Science. Transformation.™