

CYBERSECURITY REQUIREMENTS OF THE RADIO EQUIPMENT DIRECTIVE: INTRODUCING EN 18031

The Radio Equipment Directive applies to a wide range of electrical and electronic devices. Ensuring your product complies is critical to meeting EU requirements. Intertek's experts are here to help you navigate the new cybersecurity requirements.



What Are the Requirements of RED 3.3 (d), (e), and (f)?

The Radio Equipment Directive (RED) was amended to include cybersecurity requirements under Articles 3.3(d), (e), and (f), addressing network protection, privacy, and fraud prevention. These essential requirements apply to radio equipment that communicates over the internet, ensuring the protection of networks, personal data, and users from potential fraud. The Delegated Regulation (EU) 2022/30 clarifies that manufacturers must ensure their products meet these cybersecurity standards before placing them on the EU market:

- (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;*
- (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;*
- (f) radio equipment supports certain features ensuring protection from fraud.*

Scope of RED 3.3(d), (e), and (f)

It is important to know when the RED cybersecurity requirements will apply to your product:

- **Network Protection (3.3(d)):** Applies to any internet-connected radio equipment capable of exchanging data, directly or via intermediate devices.
- **Privacy (3.3(e)):** Covers radio equipment that processes personal data. Even without internet connectivity, it applies to devices capable of transmitting personal data, traffic data, location data, for the following types of equipment:
 - toys with radio function which also fall within the scope of Directive 2009/48/EC;
 - childcare products; and
 - products designed or intended to be worn on, strapped to, or hung from any part of the human body.
- **Fraud Prevention (3.3(f)):** Targets radio equipment enabling monetary transfers or virtual currency.

The MDR (Medical Devices Regulation) and IVDR (In Vitro Diagnostic Regulation) regulations include cybersecurity measures related to the risks mentioned in points (d), (e), and (f) of the RED. As a result, products regulated by the MDR and IVDR do not fall within the categories or classes of radio equipment which should comply with the essential requirements set out in Article 3(3), points (d), (e) and (f), of the RED.

Similarly, motor vehicles, civil aviation equipment, and electronic road toll systems also do not fall within the categories or classes of radio equipment which should comply with Article 3(3), points (e) and (f).

Timeline for Compliance with RED 3.3 (d), (e), (f)

Originally scheduled for August 1, 2024, the European Commission postponed the compliance deadline by 12 months.

Manufacturers now have until August 1, 2025, to align their products with the new RED cybersecurity requirements.

RED CYBERSECURITY: INTRODUCING EN 18031

Manufacturers should move quickly to integrate the necessary cybersecurity measures, avoiding delays that could result in costly product launch disruptions.

How Is Compliance Demonstrated?

Manufacturers can achieve compliance by applying the relevant parts of the harmonized standard, EN 18031. It should be noted that the standard was harmonized with restrictions.

When implemented completely, including restrictions, manufacturers may self-declare per Module A, but may also show compliance by engaging a Notified Body if they choose to demonstrate conformation through Module B+C (EU-Type Examination Certificate) or Module H (Full Quality Assurance) under RED Annexes.

A risk assessment is essential to ensure full compliance with the essential requirements or Article 3.3, points (d), (e), and (f), including the identification of any potential gaps based on identified risks.

Introducing EN 18031-1, -2, -3:

Current Status and Impact

The EN 18031 series of standards was specifically developed to demonstrate compliance with the RED cybersecurity requirements. There are three parts to the EN 18031 series of standards:

- EN 18031-1 covers network protection (Article 3.3(d)),
- EN 18031-2 addresses privacy (Article 3.3(e)), and
- EN 18031-3 focuses on fraud prevention (Article 3.3(f)).

The standard was harmonized, but it was cited in the Official Journal of the European Union with restrictions:

- Clauses 6.2.5.1 and 6.2.5.2 allow users to not set or not use passwords, which does not align with the requirements of Article 3(3), points (d), (e) and (f)
- Some categories of access control mechanisms may be incompatible with parental controls for toys and childcare radio equipment. Failure to implement parental controls would leave the authentication risks unaddressed under Article 3(3), point (e)



- The four implementation categories for secure updates are not sufficient on their own to protect financial assets under Article 3(3), point (f).

Steps Manufacturers Should Take Today

Manufacturers should act quickly to limit their risk. Here's how to get started:

- Perform a cyber risk assessment and implement a risk management process to systematically mitigate identified risks.
- Select an appropriate standard for compliance. The EN 18031 series is recommended as it directly addresses the RED Articles 3(3) d), e), and f). Alternatively, other standards such as ETSI EN 303 645 or IEC 62443 may apply, but gaps must be addressed.
- Develop technical documentation to demonstrate compliance with these standards.
- Start testing early to avoid unexpected delays. Testing ensures the products meet the requirements of the selected standard(s).
- Optionally or when necessary, engage with a Notified Body for assessment and approval under the RED.

How Intertek Can Help

At Intertek, our expertise goes beyond basic compliance. We provide tailored services, supporting every stage of your RED compliance journey, from initial risk assessments and documentation to gap analysis and independent testing. Our global team of experts and years of experience mean we're uniquely positioned to fast-track your RED compliance and guide you through certification with standards like EN 18031, ETSI EN 303 645, and IEC 62443.

Contact our team now to ensure your product is market-ready by August 2025.

FOR MORE INFORMATION



Americas
+1 800 WORLDLAB (967 5352)
+1 251 459 6173

Europe
+44 1372 370900

Asia
+852 2173 8888



icenter@intertek.com



[Intertek.com/cybersecurity](https://www.intertek.com/cybersecurity)