Radio Equipment Directive Cybersecurity Testing – EN 18031

Your guide to achieving market access into the EU for your connected devices

Why the Radio Equipment Directive and EN 18031 matters

The Radio Equipment Directive (RED, EU Directive 2014/53/EU) establishes a regulatory framework for placing radio equipment on the market in the EU. All radio equipment within the scope of this directive must comply with it as of 13 June 2017.

To enhance the cybersecurity of certain radio products in the European Union (EU) market, the European Commission has adopted a Delegated Act (Regulation (EU) 2022/30) under the RED, which takes effect on **1 August 2025**.

This Delegated Act enforces the following essential requirements from Article 3 of the RED:

- 3.3(d): Ensure network protection – radio equipment must not harm the network or its functioning nor misuse network resources.
- 3.3(e): Incorporate safeguards to ensure the personal data and privacy of the user and subscriber are protected.
- 3.3(f): Include features to protect against fraud.

These requirements ensure network protection, safeguard personal data, and prevent fraud, providing a robust foundation for safer and more secure devices in the EU market.

The EN 18031 series of standards has been published to address these essential cybersecurity requirements. Manufacturers of connected devices can use these standards to demonstrate conformity with the new RED requirements and best practices in product cybersecurity.

How BSI supports the Radio Equipment Directive and EN 18031 standards compliance

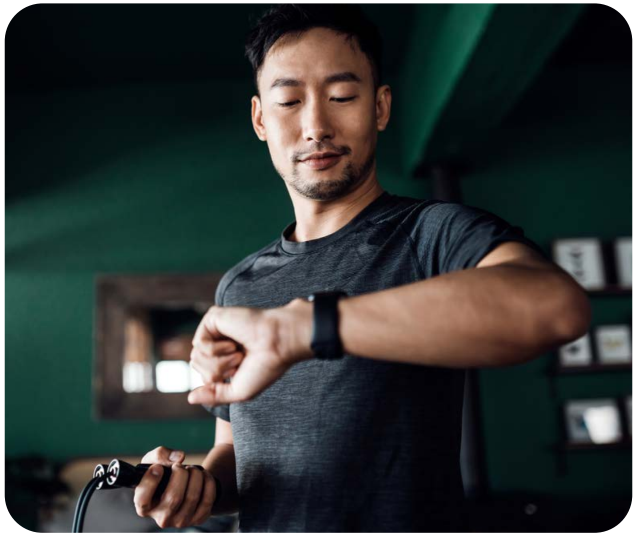
BSI is a global leader in product testing and certification services. Building on our established expertise in testing connected devices against cybersecurity standards such as ETSI EN 303 645 and ETSI TS 103 701, we now help manufacturers test their products against the stringent requirements of the EN 18031 standards.

With state-of-the-art testing facilities, skilled personnel, and extensive experience in cybersecurity testing, BSI ensures manufacturers achieve compliance with the new cybersecurity requirements of the Radio Equipment Directive through EN 18031 testing.

What to expect from this guide

This guide is tailored to help manufacturers of connected devices meet the RED market access requirements for the EU and navigate the EN 18031 compliance testing process. It includes:

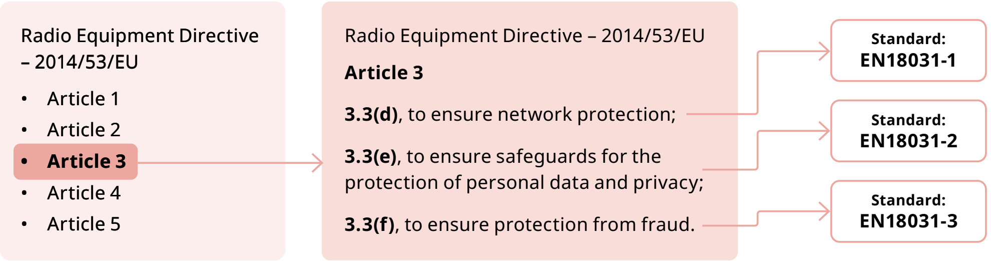
- An overview of the EN 18031 standards and their significance.
- A breakdown of typical products requiring compliance.
- Insights into BSI's specialized EN 18031 testing and certification capabilities.
- A FAQ section addressing common manufacturer concerns.
- A practical readiness checklist to assess your compliance status for the EN 18031 standards.



What are the EN 18031 standards?

Published by the European Committee for Standardization (CEN) and CENELEC in August 2024, the EN 18031 standards establish cybersecurity requirements for radio equipment aligned with the RED's essential requirements under Articles 3.3(d), (e), and (f).

These standards were harmonized with restrictions in January 2025 by the European Commission by means of the Commission Implementing Decision (EU) 2025/138 and published in the Official Journal of the European Union.



Radio Equipment Directive – 2014/53/EU

- Article 1
- Article 2
- **Article 3**
- Article 4
- Article 5

Radio Equipment Directive – 2014/53/EU

Article 3

3.3(d), to ensure network protection;

3.3(e), to ensure safeguards for the protection of personal data and privacy;

3.3(f), to ensure protection from fraud.

Standard: EN18031-1

Standard: EN18031-2

Standard: EN18031-3

EN 18031 Standards Overview

EN 18031-1: Network Protection

Ensures devices prevent harm to network infrastructure, avoid disruptions, and mitigate resource misuse, including resilience against denial-of-service attacks and unauthorized access.

EN 18031-2: Data Protection

Focuses on safeguarding personal data and user privacy through encryption, robust authentication, and controls against unauthorized access or interception.

EN 18031-3: Fraud Prevention

Addresses risks of unauthorized monetary transactions with secure transaction protocols, fraud detection mechanisms, and protection against payment system breaches.

EN 18031 security mechanisms

Each standard includes security mechanisms, detailed guidance, documentation requirements, evaluation frameworks, and functional test protocols. While overlapping in many areas, mechanisms and requirements can differ between standards, reflecting the unique focus of each.

EN 18031 -1	EN 18031 -2	EN 18031 -3	
ACM	**ACM**	**ACM**	Access control
AUM	**AUM**	**AUM**	Authentication
SUM	**SUM**	**SUM**	Secure update
SSM	**SSM**	**SSM**	Secure storage
SCM	**SCM**	**SCM**	Secure communication
RLM			Resilience
NMM			Network monitoring
TCM			Traffic control
	LGM	**LGM**	Logging
	DLM		Deletion
	UNM		User notification
CCK	**CCK**	**CCK**	Confidential cryptographic keys
GEC	**GEC**	**GEC**	General equipment capabilities
CRY	**CRY**	**CRY**	Cryptography

What products may require EN 18031 testing?

To access the EU market, manufacturers must ensure that their radio equipment complies with the EN 18031 standards if their devices are internet-connected, process personal data, or enable monetary transactions. Key product categories include:

Consumer electronics:

- Smartphones, tablets, and laptops with wireless communication capabilities.
- Smartwatches, fitness trackers, and other wearables that process and communicate personal data.
- Wireless headsets and portable media devices.

IoT and smart devices:

- Smart home products (e.g., thermostats, security cameras, smart locks, lighting systems).
- Connected appliances like smart refrigerators, washing machines, and ovens.
- Wearable health monitors, including fitness bands and heart rate monitors.
- IoT-enabled industrial equipment for monitoring or automation.

Digital and connected fire equipment:

- IoT-enabled fire alarms and smoke detectors.
- Smart fire suppression systems integrated with building platforms.
- Wireless-enabled emergency lighting systems.

Payment and financial devices:

- Wireless payment terminals used in retail and hospitality.
- Smart card readers, contactless payment devices, and mobile point-of-sale (mPOS) systems.
- Cryptocurrency transaction devices using NFC or wireless protocols.

Entertainment and educational products:

- Connected toys with radio functionality (e.g., drones and remote-controlled vehicles).
- Gaming consoles, VR headsets, and internet-connected accessories.
- E-readers and educational devices with wireless capabilities.

Transportation, automotive, and safety devices:

- Vehicle telematics, GPS trackers, and fleet management devices.
- In-vehicle infotainment systems (IVI).
- Remote keyless entry (RKE) and tire pressure monitoring systems (TPMS).

Communication and networking devices:

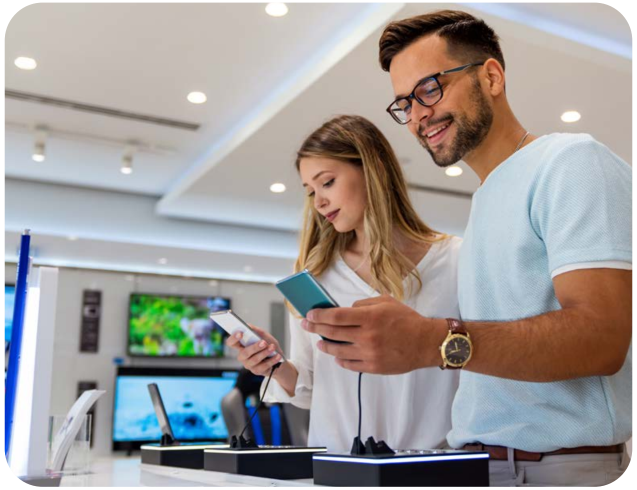
- Wi-Fi routers, access points, and mesh network devices.
- Bluetooth beacons and Zigbee-enabled smart hubs.
- Internet-connected walkie-talkies and two-way radios.

Miscellaneous connected devices:

- Baby monitors with video or audio streaming.
- Electronic pet trackers and smart collars.
- Smart wearable accessories like connected glasses, rings, and jewellery.

Products exempted from RED cybersecurity requirements

- Non-connected radio equipment (e.g., standalone two-way radios without internet capability).
- Devices used solely for military applications.
- Equipment regulated under specific sectoral frameworks (e.g., civil aviation or automotive systems).
- Medical devices covered by EU Medical Device and In-Vitro Diagnostic Medical Device Regulations.



How can BSI help me comply with RED and EN 18031?

With a long-standing heritage in product cybersecurity testing, BSI is a trusted authority in verifying compliance and ensuring product quality and security. Our extensive experience in testing internet-connected devices enables us to deliver precise and comprehensive cybersecurity testing, helping manufacturers meet the EN 18031 standards efficiently and effectively.

BSI’s advanced laboratories are equipped to assess devices against all three EN 18031 standards, providing manufacturers with:

- **Conformity testing:** Rigorous evaluations to ensure devices meet EN 18031 requirements.
- **Gap analysis:** Identification of areas of non-compliance.

Key benefits of partnering with BSI

BSI offers several benefits for manufacturers, including:

- **Expertise in product compliance:** Decades of experience testing and certifying products for global markets.
- **Technical support:** Dedicated guidance through every stage of the compliance process.
- **Efficient market access:** Streamlined processes to help manufacturers achieve RED and EN 18031 EU market entry requirements.
- **Local European presence:** Enabling us to keep up to date with the latest EU regulations and market access requirements.
- **Trusted by industry leaders:** BSI has worked with leading connected device brands, including BT and Ring, to deliver market access testing and certification.

What should I do now?

To prepare effectively for 1 August 2025, follow these steps:

1. **Identify affected products:** Determine which products in your portfolio are covered by the RED – use our checklist below to help.
2. **Conduct cybersecurity risk assessments:** Update or create cybersecurity risk assessments, focusing on the RED essential requirements (articles 3.3(d), (e), and (f)).
3. **Determine applicable requirements:** Identify which essential requirements apply to your products.
4. **Ensure compliance:** Verify that your products comply with relevant standards, such as the EN 18031 series, and prepare the necessary documentation.
5. **Obtain evidence of compliance:** Have your products tested with BSI to gather the documentation and evidence needed for your CE marking technical file.

FAQs: Understanding RED and EN 18031

What is EN 18031, and why is it important?

EN 18031 is a series of standards that can be used to demonstrate compliance with the new essential cybersecurity requirements of the RED. These standards provide a means to ensure devices are secure, protect user data, and prevent fraud. Compliance with the new RED cybersecurity essential requirements will be mandatory for in-scope devices seeking market access in the EU starting 1 August 2025.

How do I demonstrate compliance?

Compliance is typically achieved by applying harmonised standards. EN 18031-1, EN 18031-2, and EN 18031-3 were harmonised by the European Commission in January 2025. Manufacturers are required to carry out conformity testing, maintain detailed technical documentation, involve a RED Notified Body if necessary, and prepare a Declaration of Conformity. Once harmonised, these standards provide a presumption of conformity with the relevant requirements.

What happens if a product fails to comply?

Placing non-compliant products on the market can result in market bans, product recalls, penalties, and reputational damage. Manufacturers must meet applicable RED cybersecurity requirements to secure or retain CE marking for access to the EU market.

Penalties for non-compliance vary by EU member state but may include:

- Seizure of non-compliant products.
- Fines.
- Product withdrawal from the market.
- Damage to brand reputation.

Will I need a Notified Body for certification?

The EN 18031 standards have been harmonized. When these standards are applied in full, they provide automatic presumption of conformity with the relevant essential requirements, meaning the involvement of a Notified Body is not required.

However, the involvement of a Notified Body will still be necessary for many products. Manufacturers can expect future revisions of EN 18031 to address these remaining gaps.

When do the RED cybersecurity essential requirements come into effect?

The requirements become mandatory on 1 August 2025. Manufacturers should act now to prepare their products for compliance.

How can BSI support EN 18031 compliance?

BSI provides end-to-end services, including gap analysis, testing, certification, and ongoing guidance. Our state-of-the-art facilities and expert teams ensure manufacturers can meet the requirements efficiently or identify and address any gaps.

EN 18031/Radio Equipment Directive preparation checklist

Use this checklist to assess your readiness for EN 18031 compliance and to meet the requirements of the EU RED Delegated Act. Each item corresponds to a key compliance area or action required for market access by 1 August 2025.

Step 1: Product identification

1 Have you identified all radio equipment in your product portfolio?

Yes □ No □

2 Does your equipment connect to the internet (directly or indirectly)?

Yes □ No □

3 Does your equipment process personal data, traffic data, or location data?

Yes □ No □

4 Does your equipment enable monetary transactions (e.g., payments, cryptocurrency)?

Yes □ No □

Step 2: Product cybersecurity risk assessment

5 Have you conducted a product cybersecurity risk assessment for each affected product?

Yes □ No □

6 Have you documented the risks and implemented mitigation strategies?

Yes □ No □

7 Are your products designed to prevent harm to network infrastructure (e.g., protection against denial-of-service attacks)?

Yes □ No □ Not applicable □

8 Have you implemented measures to safeguard personal data and ensure privacy?

Yes □ No □ Not applicable □

9 Does your product include fraud prevention mechanisms, such as secure transaction protocols?

Yes □ No □ Not applicable □

Step 3: Compliance with EN 18031 standards

10 Have you identified the applicable EN 18031 standards for your products:

- EN 18031-1: Applicable □ Not applicable □
- EN 18031-2: Applicable □ Not applicable □
- EN 18031-3: Applicable □ Not applicable □

11 For each requirement, have you determined the compliance path using the decision tree for that requirement?

Yes □ No □

12 For each requirement, have you prepared the necessary documentation?

Yes □ No □

Step 4: Testing and validation

13 Have you conducted a gap analysis to identify areas of non-compliance?

Yes □ No □

14 Have your products been tested for compliance with EN 18031 standards?

Yes □ No □

15 Have you addressed all non-compliance gaps identified during testing?

Yes □ No □

16 Do you have evidence of compliance, including test results and technical documentation?

Yes □ No □

Step 5: Documentation and certification

17 Have you prepared a Declaration of Conformity for each compliant product?

Yes □ No □

18 Have you affixed the CE marking to all compliant products?

Yes □ No □

19 If standards are not fully applied, have you engaged a Notified Body for certification?

Yes □ No □

Step 6: Ongoing compliance

20 Do you have a process to monitor updates to EN 18031 standards and RED requirements?

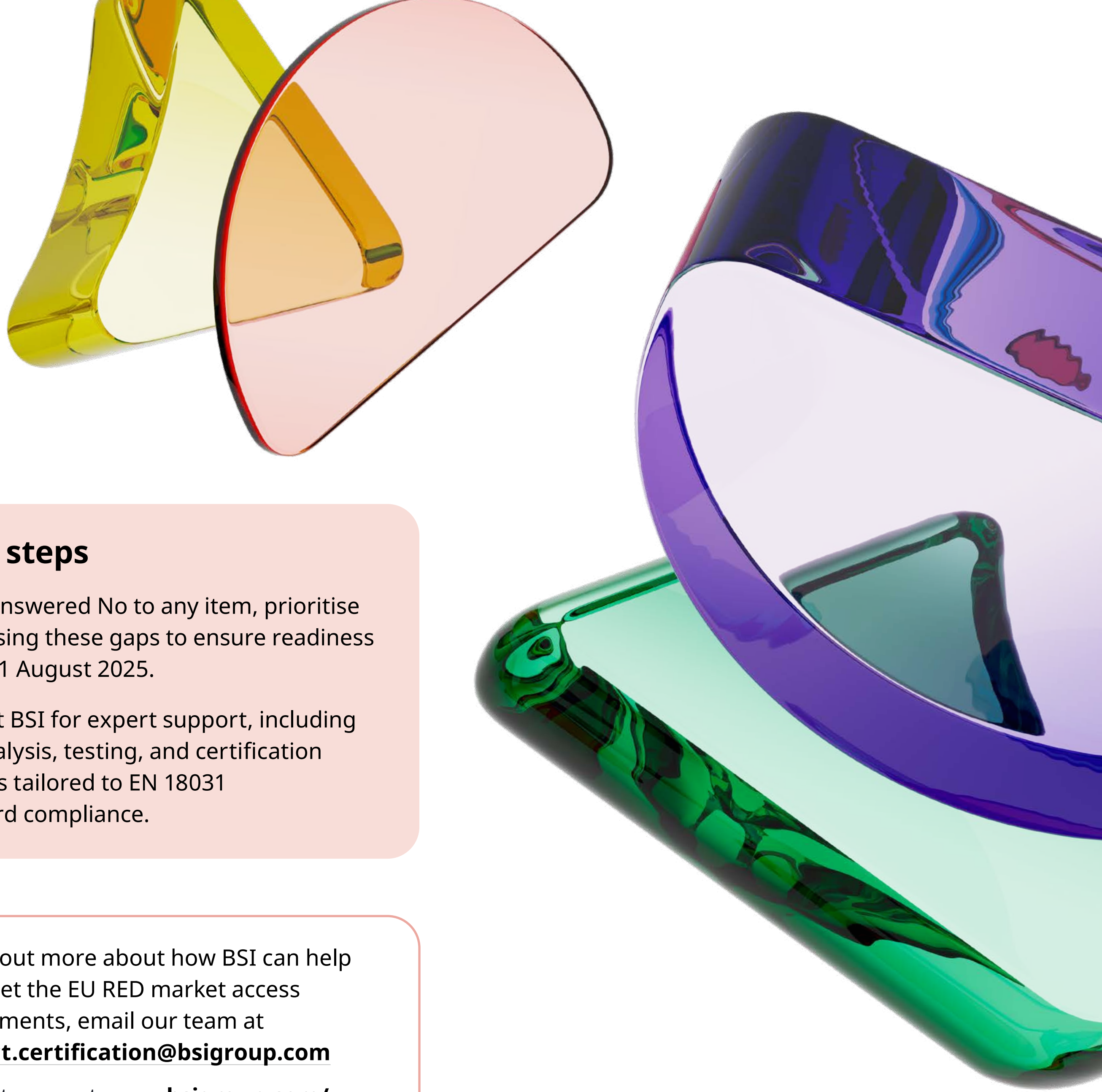
Yes □ No □

21 Are your product cybersecurity risk assessments updated regularly?

Yes □ No □

22 Have you partnered with a trusted testing and certification body, such as BSI?

Yes □ No □



Next steps

If you answered No to any item, prioritise addressing these gaps to ensure readiness before 1 August 2025.

Contact BSI for expert support, including gap analysis, testing, and certification services tailored to EN 18031 standard compliance.

To find out more about how BSI can help you meet the EU RED market access requitements, email our team at **product.certification@bsigroup.com**

Find out more at **www.bsigroup.com/radio-equipment-directive**

BSI Group, Kitemark Court, Davy Avenue,
Knowlhill, Milton Keynes, MK5 8PP