Getting Ready for the EU Radio Equipment Directive:

Ensuring Cybersecurity Compliance for Market Access

A BSI webinar

11th March 2025

Hello and welcome

- In this webinar we'll introduce the EU Radio Equipment Directive (RED), including:
  - What it is
  - Which products need to comply with RED
  - Which products are exempt
  - What you need to do to be ready for the 1st August deadline
  - RED services BSI offers to help ensure you keep your EU market access
- Q+A at the end of the webinar – please add your questions to the chat
- You will get a copy of slides and a recording of the webinar
- Opportunity to ask for a follow up from BSI on the feedback form – available immediately after the webinar concludes.

Your free RED toolkit

- Prepare for the upcoming RED regulations with our RED toolkit, including:
  - Guide to RED regulations
  - FAQs on RED
  - 2-page checklist to assess compliance & next steps
- Visit page.bsigroup.com/bsi-red-toolkit or scan the QR code

Meet our speakers

Carlos Pérez Ruiz

Global Head of Digital Trust, Product Certification

Carlos leads BSI’s global digital trust portfolio, bringing 20 years of expertise in cybersecurity testing and certification services.

Mustanir Ali

IoT certification team manager

With over a decade of experience in CE marking, testing, and certification of software-driven products, Mustanir specialises in consumer electronics, medical devices, and more.

Cybersecurity

It’s kind of a big deal

How many questions can you get right?

Answer the public – question 1

According to NordVPN, what percentage of IoT device users do NOT take any measures to protect their devices?

- 5%
- 15%
- 25%
- 50%

Source - https://nordvpn.com/research-lab/iot-device-security/

Answer the public – question 1

According to NordVPN, what percentage of IoT device users do NOT take any measures to protect their devices?

- 5%
- 15%
- 25% ✓
- 50%

Source - https://nordvpn.com/research-lab/iot-device-security/

Answer the public – question 2

According to IoT Security Foundation, what percentage of consumers are highly concerned about the security of IoT devices?

20%

32%

56%

66%

Source - https://iotsecurityfoundation.org/what-do-consumers-think-about-iot//

Answer the public – question 2

According to IoT Security Foundation, what percentage of consumers are highly concerned about the security of IoT devices?

20%

32%

56%

66% ✓

Source - https://iotsecurityfoundation.org/what-do-consumers-think-about-iot//

Answer the public – question 3

Based on data from Security Magazine, what percentage of organizations have seen an increase in cyber attacks on their IoT devices over the past three years?

40%

55%

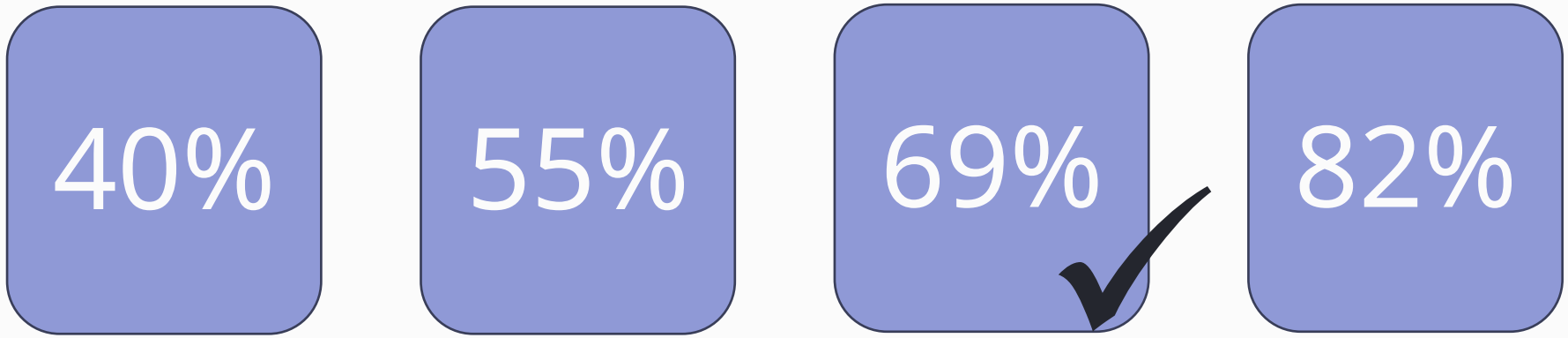
69%

82%

Source - https://www.securitymagazine.com/articles/99993-survey-97-face-challenges-securing-iot-and-connected-devices

Answer the public – question 3

Based on data from Security Magazine, what percentage of organizations have seen an increase in cyber attacks on their IoT devices over the past three years?



Source - https://www.securitymagazine.com/articles/99993-survey-97-face-challenges-securing-iot-and-connected-devices

Upcoming changes to the EU Radio Equipment Directive explained

Carlos Pérez Ruiz

What is the EU Radio Equipment Directive?

- The EU Radio Equipment Directive 2014/53/EU (RED) establishes a regulatory framework for placing radio equipment on the market in the EU. All radio equipment within the scope of this directive that are placed on the market in the EU must have been compliant with the directive from 13 June 2017.
- The Directive applies to all equipment that emits or receives radio waves **for radiodetermination** or **communication purposes**.
- **This includes devices such as mobile phones, laptops, smart devices, automotive connected devices and many more.** It does not cover radio equipment used for **public security and defence** activities, or radio equipment used by **radio amateurs**.
- The RED defines **essential requirements**:

Essential Requirements			
Article 3.1(a) Health & Safety of the user and animals, but no voltage limit applying **[Equivalent to LVD]**	**Article 3.1(b)** Adequate level of Electromagnetic Compatibility (EMC) **[Equivalent to EMCD]**	**Article 3.2** Efficient use of radio spectrum in order to avoid harmful interference (RF)	**Article 3.3 Cybersecurity** 3.3(d) Protection of the network 3.3(e) Protection of personal data and privacy 3.3(f) Protection from fraud

What is RED Commission Delegated Regulation (EU) 2022/30?

- The EU Radio Equipment Directive (RED) 2014/53/EU came into effect in June 2017
- **The Commission Delegated Regulation (EU) 2022/30 of October 29, 2021 applies cybersecurity essential requirements to 'internet-connected radio equipment'** beginning 1 August 2025

3.3(d) Radio equipment doesn't harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service

3.3(e) Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and the subscriber are protected

3.3(f) Radio equipment supports certain features ensuring protection from fraud

What is RED Commission Delegated Regulation (EU) 2022/30?

- Certain product types are excluded from the scope of the delegated act

Article 3.3(d), (e) and (f) do **not** apply to:

- Medical devices
- IVD medical devices

Article 3.3(e) and (f) do **not** apply to:

- Civil aviation equipment
- Automotive equipment
- Electronic road toll systems

- In addition, Article 3.3(e) of the RED applies to wearable radio equipment, toys which are also radio equipment, and radio equipment for childcare, whether internet-connected or not

shall avoid any hazards related to

- remote communication
- observation and control of the child
- unauthorised communications or interactions to their user

What products may require RED 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.

EV chargers with internet connectivity

- Smart EV charging stations with network capabilities for remote monitoring and control.
- Connected home and commercial EV chargers that transmit data over Wi-Fi, Bluetooth, or cellular networks.
- Payment-enabled public EV charging stations requiring secure transaction protocols.
- Fleet management EV chargers with IoT integration for energy monitoring and reporting.

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.

Why is this RED update important?

From 1 August 2025, all radio equipment covered by these essential requirements must comply in order to be placed onto the EU market

- Products currently being placed on the market will need to comply if they will continue to be placed on the market after this date
- Compliance with applicable essential requirements will be required for CE marking

CE

- Some products are placed on the UK market using CE marking, this will apply to these products too!
- RED compliance does **not** replace the PSTI

How to comply

Module A

Internal Production Control

‘self declaration’

Module B + C

EU-type examination +

Conformity to type based on internal production control

Module H

Conformity based on full quality assurance

Where, in assessing the compliance of radio equipment with the essential requirements, the manufacturer has applied **harmonised standards** any of these procedures may be used

How to comply

Module B + C

EU-type examination +

Conformity to type based on internal production control

Notified body required

Module H

Conformity based on full quality assurance

Where, in assessing the compliance of radio equipment with the essential requirements, the manufacturer either

- **has not** applied harmonised standards;
- has applied **only in part** harmonised standards;
- or where harmonised standards **do not exist**

only these procedures may be used

Harmonized standards

- The European Commission asked CEN and CENELEC to develop harmonized standards
  - EN 18031-1 covers ER 3.3(d) protection of the network
  - EN 18031-2 covers ER 3.3(e) protection of personal data and privacy
  - EN 18031-3 covers ER 3.3(f) protection from fraud
- These standards were published in August 2024
- They were harmonized (with restrictions) in January 2025

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

BSI services for RED compliance

Radio equipment testing to EN 18031 standards

- Conceptual evaluation
- Functional evaluation
- Testing location: Hemel Hempstead, UK

- EU notified body for RED essential requirements 3.3(d), (e), (f) application in process

Our Internet of Things testing laboratory in Hemel Hempstead, UK is the first and only UKAS-accredited laboratory for cybersecurity testing of connected devices

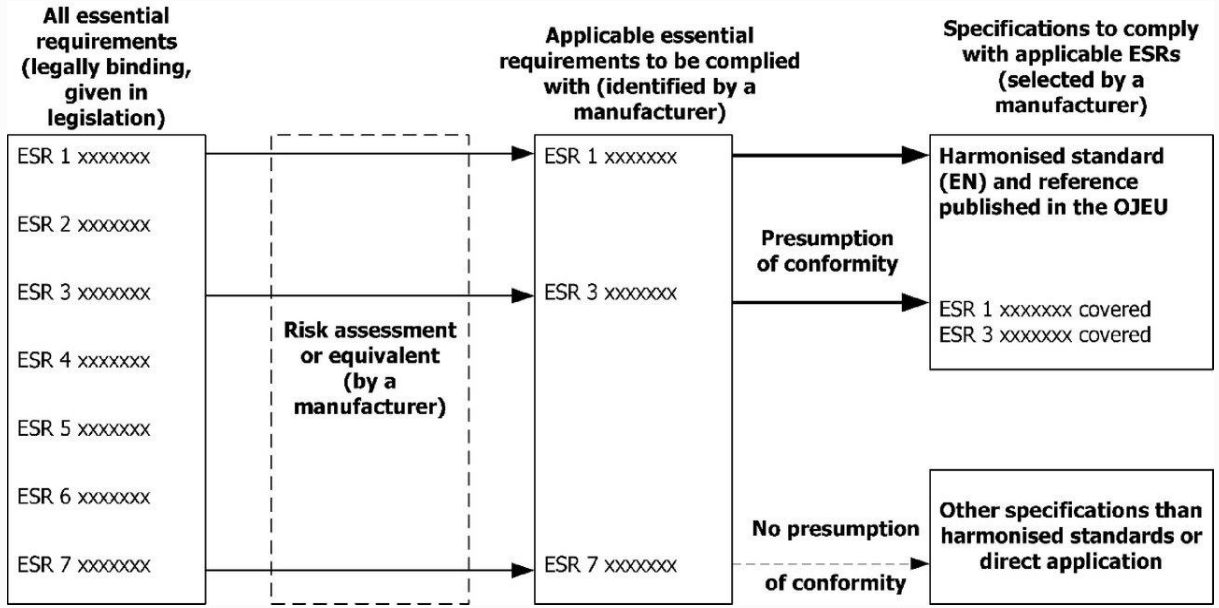
ISO/IEC 17025
ETSI EN 303 645
ETSI TS 103 701

An introduction to the EN 18031 standards

Mustanir Ali

How can I get ready for the RED?

- Review product risk assessment(s)
  - Is your product in scope?
  - Which essential requirements are applicable?
- Start applying technical solutions
  - EN 18031-1/2/3 to cover applicable essential requirements
  - Use existing IoT product cybersecurity standards such as ETSI EN 303 645 and EN 62443-4-2?
- Apply conformity assessment procedure
  - Product testing
  - Use notified body?



Source: The 'Blue Guide' on the implementation of EU product rules 2022/C 247/01

EN 18031 - mechanisms

EN 18031 -1	EN 18031 -2	EN 18031 -3
ACM	ACM	ACM
AUM	AUM	AUM
SUM	SUM	SUM
SSM	SSM	SSM
SCM	SCM	SCM
RLM		
NMM		
TCM		
	LGM	LGM
	DLM	
	UNM	
CCK	CCK	CCK
GEC	GEC	GEC
CRY	CRY	CRY
33	43	37

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

EN 18031 - assets

Asset – information, data or function that is to be protected – see Annex A.2.6 of the standards

Confidential – disclosure may lead to harm

Sensitive – manipulation may lead to harm

EN 18031-1

- Network asset
  - Sensitive network function configuration
  - Confidential network function configuration
  - Network function

EN 18031-2

- Privacy asset
  - Sensitive personal information
  - Confidential personal information
  - Sensitive privacy function configuration
  - Confidential privacy function configuration
  - Privacy function

EN 18031-3

- Financial asset
  - Sensitive financial data
  - Confidential financial data
  - Sensitive financial function configuration
  - Confidential financial function configuration
  - Financial function

- Security asset
  - Sensitive security parameter
  - Confidential security parameter
  - Security function

How to use EN 18031

EN 18031-1/2/3

[AUM-5] Password Strength
- [AUM-5-1] Requirement
- Rationale
- Guidance
- Assessment criteria
  - Assessment objective
  - Implementation categories
  - Required Information

Implementation categories:

[IC.AUM-5-1.UniqueBestPractice]
[IC.AUM-5-1.EnforceSettingFirstUse]

How to use EN 18031

EN 18031-1/2/3

[AUM-5] Password Strength
- [AUM-5-1] Requirement
- Rationale
- Guidance
- Assessment criteria
  - Assessment objective
  - Implementation categories
  - Required Information

Required information:

[E.Info.AUM-5-1.AUM]
Description of each authentication mechanism using factory default passwords

[E.Info.AUM-5-1.AUM.PwdProperty]
For each authentication mechanism's factory default password, explanation of how it complies with the requirement

[E.Info.DT.AUM-5-1]
Description of path through the decision tree

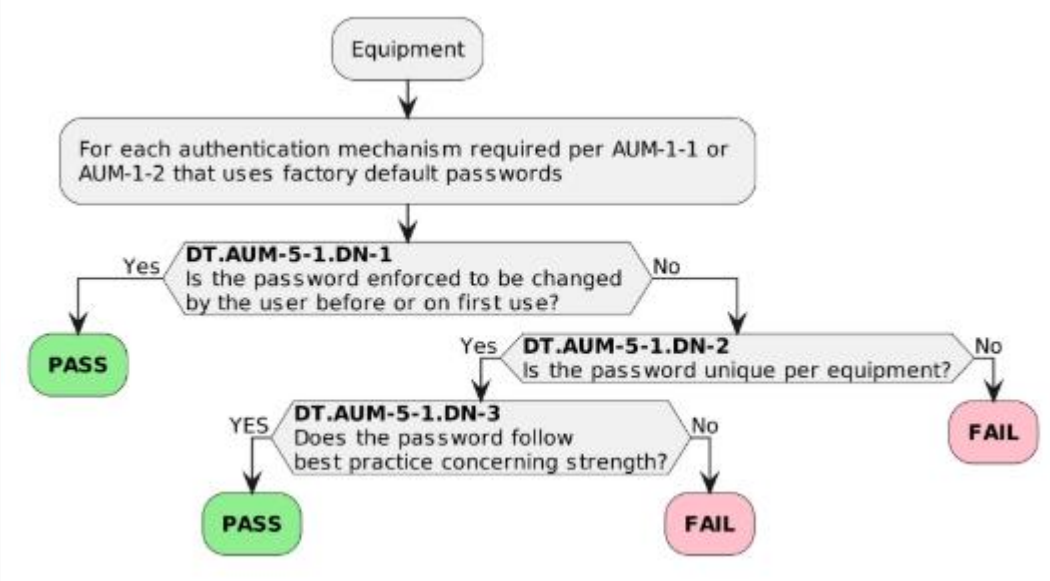
[E.Just.DT.AUM-5-1]
Justification of path through the decision tree

Assessing compliance with EN 18031

EN 18031-1/2/3

[AUM-5] Password Strength
- [AUM-5-1] Requirement
- Rationale
- Guidance
- Assessment criteria

- Assessment objective
- Implementation categories
- Required Information
- Conceptual Assessment
  - Does the required information and rationale make sense?
  - Decision tree

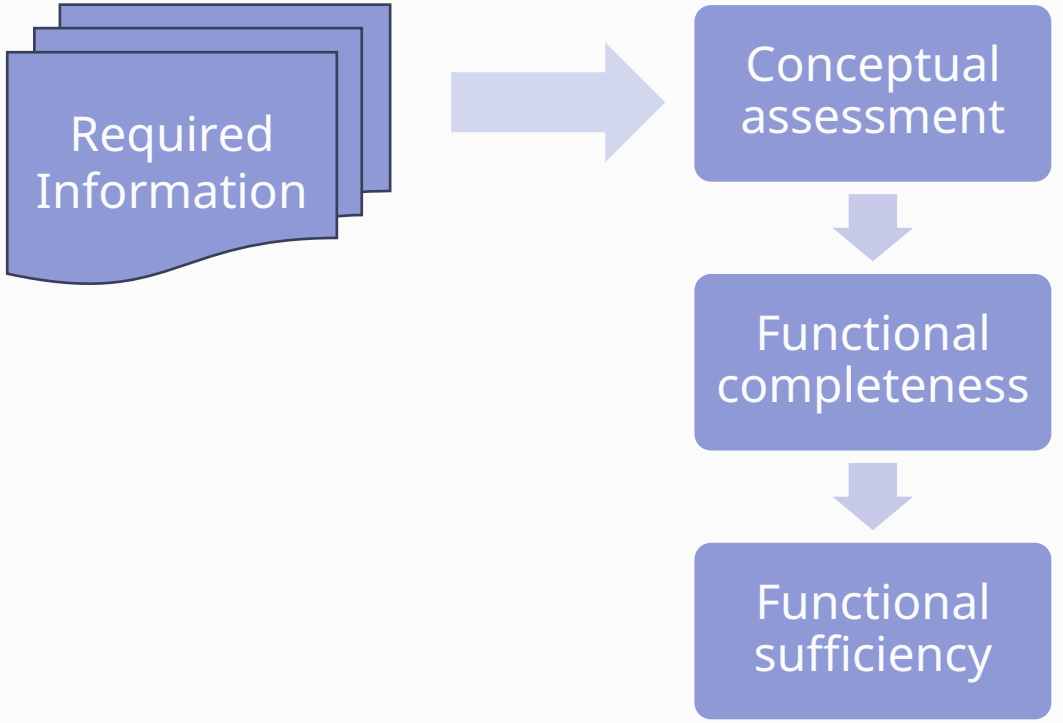


Assessing compliance with EN 18031

EN 18031-1/2/3

[AUM-5] Password Strength
- [AUM-5-1] Requirement
- Rationale
- Guidance
- Assessment criteria

- Assessment objective
- Implementation categories
- Required Information
- Conceptual Assessment
  - Does the required information and rationale make sense?
  - Decision tree
- Functional completeness assessment
  - Is the information provided complete?
- Functional sufficiency assessment
  - Is the implementation adequate?



EN 18031 – harmonization restrictions

EN 18031 standards may be considered as harmonized standards, with certain restrictions

Notice 1:

The sections named ‘rationale’ and ‘guidance’ do not confer presumption of conformity

Notice 2:

The standards do not provide presumption of conformity if, when applying clauses 6.2.5.1 and 6.2.5.2 (password strength) the user is allowed to *not set and use any password*

EN 18031-2 – harmonization restrictions

Notice 3: For certain classes of radio equipment, this standard does not provide presumption of conformity if parental or guardian access control is not ensured

Affected products

- Toys
- Childcare equipment

Affected requirements

[ACM-3] Default access control for children in toys

[ACM-4] Default access control to children’s privacy assets

[ACM-5] Parental/Guardian access control for children in toys

[ACM-6] Parental/Guardian access controls for other entities’ access to managed children’s privacy assets in toys

EN 18031-3 – harmonization restrictions

Notice 3: The assessment criteria of clause 6.3.2.4 [SUM-2] do not provide presumption of conformity

[SUM-2] Requirement

Each update mechanism shall only install software whose integrity and authenticity are valid at the time of installation

6.3.2.4 Assessment criteria

- 4 implementation categories:
  - Digital signatures
  - Secure communication
  - Access control + hash-protected software update
  - Something else

‘None of these methods alone are considered sufficient for the treatment of financial assets’

Commission Implementing Decision (EU) 2025/138 of 28 January 2025

Next steps

- Identify which RED essential requirements apply to your products
- Decide which standards to apply and get hold of your copies
- Review your product against the requirements
- Prepare the information required
- Submit your product for assessment
- Apply to a notified body?

RED readiness checklist – available via BSI RED Toolkit

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 ☐

Download your free checklist via the RED toolkit

Visit page.bsigroup.com/bsi-red-toolkit or scan the QR code

Any questions for our speakers?

Carlos Pérez Ruiz

Global Head of Digital Trust, Product Certification

Mustanir Ali

IoT certification team manager

Download your free RED toolkit

Visit page.bsigroup.com/bsi-red-toolkit or scan the QR code

Thanks for joining

Find out more or enquire about our EN 18031 services at

bsigroup.com/radio-equipment-directive

Download your free checklist via the RED toolkit, visit

page.bsigroup.com/bsi-red-toolkit

or scan the QR code

Want to talk about RED product testing with our team, request via our feedback form or email

product.certification@bsigroup.com

with the subject ‘Query following BSI Radio Equipment Directive webinar’