Qity

A PLAYBOOK FOR CONNECTED RADIO EQUIPMENT

Cybersecurity under the Radio Equipment Directive, and how EN 18031 is applied

Since 1 August 2025 the cybersecurity essential requirements of Directive 2014/53/EU apply to specified classes of connected radio equipment, and EN 18031-1, EN 18031-2 and EN 18031-3 are the harmonised standards cited for them. This playbook works through what those standards actually ask of a manufacturer, what the Official Journal restrictions do to the conformity assessment route, and where Annex II internal production control stops being available. It ends with the assessment Qity gives manufacturers to separate a remediable evidence gap from a legal trigger for a Notified Body.

Three essential requirements, three standards

Commission Delegated Regulation (EU) 2022/30 activates Article 3(3)(d), (e) and (f) of the RED for specified categories of radio equipment, and as amended by Delegated Regulation (EU) 2023/2444 those requirements have applied since 1 August 2025. Implementing Decision (EU) 2025/138 cites the EN 18031:2024 series in the Official Journal, with restrictions that are material to the route rather than cosmetic.

> *"Applying EN 18031 to a specific product is the manufacturer's responsibility."*
> European Commission guidance on the EN 18031 restrictions

3(3)(D) · EN 18031-1

Protection of the network

Applies to any radio equipment that can reach the internet, directly or through a phone, gateway or router, so it is not limited to products with their own modem. The concern is the equipment becoming a source of harm: retry loops, excessive traffic, abused exposed services and compromised update channels.

3(3)(E) · EN 18031-2

Personal data and privacy

Applies to internet-connected equipment, childcare equipment, toys under the Toy Safety Directive and specified wearables that process personal, traffic or location data. Identifiers, credentials, audio, telemetry and logs count once they can be linked to a user, and selling business-to-business excludes nothing.

3(3)(F) · EN 18031-3

Protection against fraud

Applies where internet-connected equipment enables the user to transfer money, monetary value or virtual currency. Billing through a separate enterprise system does not make a product a value-transfer product, but the non-applicability decision must state the functions examined and the trigger for revisiting it.

CYBERSECURITY IS NOT THE WHOLE RED FILE

Article 3(1)(a) health and safety, Article 3(1)(b) EMC and Article 3(2) efficient use of spectrum remain part of the same conformity assessment, and questions about antennas, modified housings, shielding or enabled bands ordinarily need a competent testing laboratory. No route conclusion follows from EN 18031 evidence alone.

A CE-MARKED MODULE IS EVIDENCE, NOT COVER

The object of assessment is the final radio equipment placed on the market under the manufacturer's name. A supplier declaration for an incorporated module or router is supporting evidence subject to integration conditions, and where a router leaves its original housing that evidence may no longer be representative.

WHICH EQUIPMENT IS CAUGHT

Caught

Anything that can reach the internet, on its own or through a phone, gateway or router. Connected sensors, cameras, wearables, appliances, industrial gateways, toys and childcare equipment, and any product that also carries a payment or virtual-currency function.

Still caught, often assumed otherwise

Equipment sold business-to-business, equipment behind a customer firewall, and equipment whose connectivity is provided by an integrated third-party module. Connectivity that is present but disabled by default is still connectivity.

Excluded

Equipment covered by the specified aviation, motor-vehicle and medical-device exclusions in Delegated Regulation (EU) 2022/30, and equipment with no internet reachability at all. Both need a written determination, not an assumption.

THE COMPLIANCE WINDOW

30 JAN 2025

EN 18031 series cited

Implementing Decision (EU) 2025/138 cites the three parts in the Official Journal, with the four restrictions attached.

1 AUG 2025

Requirements apply

Articles 3(3)(d), (e) and (f) are enforceable for products placed on the EU market from this date, with no transition for new placements.

11 DEC 2027

CRA supersedes

Delegated Regulation (EU) 2022/30 is repealed and the Cyber Resilience Act applies in full, extending the obligations beyond radio equipment.

What a successful assessment finds in the product

EN 18031 names mechanisms; conformity is carried by the controls behind them, decided per assessment unit rather than once for the product.

01 · IDENTITY AND ACCESS — ACM · AUM

No shared or default secrets

- A unique per-unit credential set at production, or forced enrolment on first use, never a printed common password.
- Authentication on every external interface: debug, serial, local web, BLE pairing and cloud API.
- Least-privilege roles, with factory and remote-support accounts removed or individually controlled.
- Rate limiting or lockout against brute force, and session state that cannot be replayed.

02 · SOFTWARE INTEGRITY — SUM · GEC

Only signed code runs, and stays running

- Firmware signature verified before installation, with the trust anchor where it cannot be rewritten.
- Anti-rollback so a withdrawn version cannot return, and safe recovery from an interrupted update.
- Signing key in an HSM with named approvers, and a revocation path if it is compromised.
- A declared support period and a route to reach fielded units with a security fix.

03 · DATA IN TRANSIT — SCM · CRY

Authenticated channels, not just encrypted

- Endpoint identity verified: chain, hostname and expiry checked, pinned where deployment allows.
- Current cipher suites and protocol versions, with downgrade and plaintext fallback refused.
- Replay protection, and failure behaviour that stops rather than continues when validation fails.
- The same treatment for BLE, Wi-Fi provisioning and LAN paths, which are in scope too.

04 · DATA AT REST — SSM · CCK

Assets classified, keys held properly

- An inventory of stored assets marking what needs confidentiality, integrity or both.
- Credentials, tokens and personal data protected in flash and backups, not in a debug partition.
- Keys separated by purpose: trust anchor, device identity, transport, backend and test never shared.
- Qualified entropy at generation, with rotation, revocation and destruction defined per key.

05 · EXPOSURE AND RESILIENCE — GEC · RLM · NMM · TCM

A small, known and stable attack surface

- A documented baseline of exposed ports and services, with anything unneeded disabled in production.
- Optional services user-configurable, and no undocumented interface left enabled after manufacturing.
- Input validation and defined behaviour under malformed traffic and resource exhaustion.
- Rate and retry limits so the equipment cannot become a source of network harm.

06 · PRIVACY AND DISCLOSURE — LGM · DLM · UNM

User-facing control over their data

- Persistent security logging with the required events and reliable time information.
- A working deletion path for personal data on device, in the application and in the backend.
- Notification to the user on collection and on security-relevant change, in the required content.
- A disclosure contact and triage process, with known exploitable vulnerabilities fixed before release.

A CONTROL IS ONLY EVIDENCE WHEN IT IS REPRODUCIBLE

Each control needs a named implementation in the declared configuration, an artefact showing it works, and a production step that reproduces it on every unit. A control shown on an engineering sample but not enforced in manufacturing does not support the declaration.

Four gates decide whether you can sign this yourself

Annex II internal production control lets the manufacturer declare conformity alone, and Article 17(4) allows it only where the cited standards are applied in full. Every gate must pass for each applicable requirement; one failure sends that requirement to Annex III or Annex IV.

THE DECISION PATH

1 Is the requirement in scope?

Decide 3(3)(d), (e) and (f) separately from product facts: internet reachability, personal data, and money or virtual-currency transfer.

Yes · Go to gate 2. **No** · Out of scope, with the functions examined recorded.

2 Does a cited standard cover it?

EN 18031-1, -2 and -3 are cited in Implementing Decision (EU) 2025/138. Check the product type and its interfaces fall inside the relevant part.

Yes · Go to gate 3. **No** · No presumption. Annex III or IV.

3 Is the standard applied in full?

Every applicable mechanism assessed by the standard's method, every assessment unit given a verdict, every not applicable decision justified.

Yes · Go to gate 4. **No** · Partial application. Annex III or IV.

4 Do the restrictions leave presumption intact?

The Official Journal restrictions withdraw presumption for specific clauses. Check each against the implementation actually chosen.

Yes · Annex II is legally available. **No** · Presumption lost. Notified Body.

Legally available is not the same as ready

Passing the gates means Article 17 permits Annex II. Whether controlled evidence exists today for each control is the separate question that usually delays the declaration.

THE FOUR OFFICIAL JOURNAL RESTRICTIONS

The password option · all three parts

Presumption is lost where clauses 6.2.5.1 and 6.2.5.2 are applied so the user may set no password at all. Commission guidance is that no third-party assessment is required if the manufacturer disregards that option, so requiring a credential on every interface keeps Annex II open. This is the most common self-inflicted trigger.

Secure update · EN 18031-3 clause 6.3.2.4

Presumption is removed for those assessment criteria, and Commission guidance states third-party conformity assessment is mandatory where the clause applies. If the product transfers monetary value, settle this before planning a self-declared release.

Parental control · EN 18031-2

Presumption is lost for the specified toy and childcare clauses where parental or guardian access control is not ensured. Establish first whether the product is inside those clauses at all.

Rationale and guidance sections

Those sections set no specifications and confer no presumption, so conclusions must be tied to the normative requirements. No third-party assessment follows from this restriction alone.

If a Notified Body is required

Only the failing requirement goes to Annex III or IV; the rest can still run under Annex II. The body must be notified for that specific requirement, its certificate must match the declared configuration, and the DoC must name the procedure actually used.

04 · WHERE QITY COMES IN

Start with the assessment, then close the gaps

The first question is not what to build, it is whether this product can still be self-declared and what is missing if it can.

START HERE · QITY.APP

The RED cybersecurity readiness assessment

Work through scope, restrictions and evidence for one product and get a structured result: which of Article 3(3)(d), (e) and (f) apply, whether the four gates pass, and which controls have no evidence behind them yet.

Run the assessment at qity.app

One product, about twenty minutes

CYBERSECURITY SERVICES FOR MANUFACTURERS *Any manufacturer of connected radio equipment, in any sector.*

Scope and applicability
Which cybersecurity requirements apply to each product and variant, argued from product facts with evidence references attached.

Full EN 18031 assessment
Every mechanism worked per assessment unit using the standard's own method and identifiers, with a verdict per case.

Control design and remediation
Hands-on work on the controls that fail: credential provisioning, signed update pipelines, key management, attack-surface reduction.

Restriction and route strategy
Clause-level analysis of the password, parental-control and 6.3.2.4 restrictions, and scoping a Notified Body submission if needed.

Technical file and declaration
The evidence package controlled so the file supports the declaration, including production controls that hold per unit.

Post-market and CRA readiness
Vulnerability monitoring, disclosure handling and update governance, so December 2027 is a continuation rather than a restart.

SIX QUESTIONS TO ASK FIRST More than two answers of no means the file does not yet support the declaration.

Boundary	Are the hardware revisions, firmware versions, applications and backend services in the declared configuration identified?	Yes / Partly / No
Applicability	Does each 3(3)(d), (e) and (f) conclusion rest on stated product facts and an evidence reference?	Yes / Partly / No
Restrictions	Is the password option addressed on every interface, and clause 6.3.2.4 checked if Part 3 applies?	Yes / Partly / No
Controls	Does every applicable control have a named implementation, an artefact proving it works, and a verdict?	Yes / Partly / No
Production	Do provisioning, credential generation, key injection and hardening reproduce the assessed configuration on every unit?	Yes / Partly / No
Declaration	Does the DoC name the cybersecurity requirements, the standards applied and the procedure actually used?	Yes / Partly / No