CRA

CRA (whole Part)

Audit Checklist

153 audit questions across **25** sections.

HOW TO USE THIS CHECKLIST

Each question has three boxes the auditor fills in during the audit:

1. **Compliance** — the binary headline: Compliant / Non-compliant.
2. **Classification** — where the gap is, four-state grid: Documented / Implemented matrix.
3. **Finding level** — severity: Maj / Min / Obs (Major nonconformity / Minor nonconformity / Observation).

Severity is the auditor's call on the day, against the real finding — no severity is pre-suggested per question.

auditchecklists.org Audit Checklist Licence

Product:	CRA (whole Part) (153 questions)
Regulation:	
Issued:	[YYYY-MM-DD — STAMPED AT ISSUE]

Licensed to:	[ORG NAME — STAMPED AT ISSUE]
Licensee email:	[EMAIL — STAMPED AT ISSUE]
Order:	[AVI-YYYY-NNNNN — STAMPED AT ISSUE]

Licence terms

This audit checklist is licensed for use within the organisation named above by the licensee email named above. Use is permitted by employees and contractors of the named organisation in the course of their work for that organisation, including printing, internal distribution within the organisation, annotation during audits, and incorporation into the organisation's management-system documentation as a working reference.

Not for redistribution. Sharing this document, or any derivative or extract of it, with any party outside the named organisation is a breach of this licence. This includes posting to file-sharing networks, internal wikis or knowledge bases accessible to other organisations, vendor portals, supplier-facing GRC systems, and email forwarding to colleagues at other firms. Quoting individual audit questions in regulator submissions or internal training materials is permitted; reproducing the structured checklist as a whole is not.

Each additional organisation or operating site requires a separate licence. If a sister organisation in the same group, or a separate operating entity, requires the same checklist, contact licences@auditchecklists.org for a multi-site licence quote. Holding companies licensing for multiple subsidiaries are eligible for group-licence pricing.

Licence transfers. This licence does not transfer with sale, merger, or organisational restructure without written consent. auditchecklists.org may, at its discretion, transfer the licence to the successor organisation on request — usually a formality, contact licences@auditchecklists.org.

Defects and amendments. If you identify a defect in this checklist — wrong content, mistranscribed regulation, factual error — email support@auditchecklists.org. We will verify the defect, correct it, and reissue the affected artefacts to you within a reasonable timeframe at no further charge. Regulatory amendments published during your 12-month update

Essential cybersecurity requirements

Q1 ANNEX CRA Annex–I.I.1

Are the entity's PWDE designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks?

SOURCE VERBATIM

> Part I Cybersecurity requirements relating to the properties of products with digital elements (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
>
> — Regulation (EU) 2024/2847 Annex I Part I (1), Original 2024-10-23 (CRA)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Per PWDE: risk-based design rationale
- Lifecycle gate evidence (design / dev / production)

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q2 ANNEX CRA Annex–I.I.2(a)

Based on the Art-13(2) cybersecurity risk assessment and where applicable, are PWDE made available on the market without known exploitable vulnerabilities?

SOURCE VERBATIM

> (a) be made available on the market without known exploitable vulnerabilities;
> — Regulation (EU) 2024/2847 Annex I Part I (2)(a), Original 2024-10-23 (CRA)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs
Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Pre-release vulnerability scan / fix log
- Per PWDE: known-vulns-at-shipping disposition

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q3 ANNEX CRA Annex–I.I.2(b)

Are PWDE made available on the market with a secure-by-default configuration — unless otherwise agreed between manufacturer and business user in relation to a tailor-made PWDE — including the possibility to reset the product to its original state?

SOURCE VERBATIM

> (b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;
>
> — Regulation (EU) 2024/2847 Annex I Part I (2)(b), Original 2024-10-23 (CRA)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Default-configuration evidence per PWDE
- Reset-to-original mechanism

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES: