NIS2 Evidence Checklist for Confluence

Compliance for Confluence + Workflows for Confluence | AppFox

NIS2 is a cybersecurity directive, not a documentation standard. This checklist covers the documented-governance, access-control and asset-management measures you can evidence inside Confluence (using Compliance for Confluence or Workflows for Confluence), plus the management-accountability evidence Article 20 demands. It does not cover NIS2's technical and incident-response obligations (see the scope note). An editable Excel tracker version for use as a working template is also available here.

NIS2 reference	Requirement (in brief)	Evidence an auditor expects	How to produce it in Confluence (app – feature)
1. Governance & accountability			
Article 20 — Management approval & oversight	Management body approves the risk-management measures and oversees implementation; is personally accountable.	Dated, named approval records for each measure.	Workflows – Approval Workflows + e-signature tokens
Article 20 — Training	Management and staff undergo regular cybersecurity training.	Acknowledgement / sign-off records for training.	Workflows – acknowledgement / sign-off workflows
2. Security policies & risk analysis			
Art. 21(2)(a) — Risk analysis & infosec policies	Maintain approved, current policies on risk analysis and information system security.	Approved, version-controlled policy set; classified and access-controlled.	Workflows – lifecycle/approval/publishing; Compliance – classification & restriction
3. Access control, HR security & asset management			
Art. 21(2)(i) — Access control	Enforce access control policies.	Classification-driven page restrictions; permission report.	Compliance – Restriction Schemes bound to Levels
Art. 21(2)(i) — Asset management	Identify and manage information assets.	Inventory/report of classified pages and owners.	Compliance – Classification Levels; Dashboard & reporting
Art. 21(2)(i) — HR security policies	Maintain and approve HR-security and access policies.	Approved policy documents, access-controlled.	Workflows – approval; Compliance – role restriction
4. Assess effectiveness			
Art. 21(2)(f) — Effectiveness review	Assess that the risk-management measures actually work.	Dated review/re-approval records; monitoring reports.	Workflows – Content Expiration / review cycles; Compliance – Dashboard
5. Incident, continuity & training docs (documentation support only)			
Art. 21(2)(b) — Incident handling (docs)	Maintain incident-response playbooks and corrective actions.	Approved IR playbooks; corrective-action workflow history.	Workflows – approval/review + corrective-action workflows
Art. 21(2)(c) — Business continuity (docs)	Maintain BC/DR and crisis-management plans.	Approved, current BC/DR plan documents.	Workflows – approval / review / expiry
Art. 21(2)(g) — Cyber hygiene & training (docs)	Provide training and record completion.	Published materials + acknowledgement records.	Workflows – publishing + acknowledgement workflows
6. Supervision & audit trail			
Supervision / audit (cross-cutting)	Demonstrate governance to national competent authorities.	Workflow history exports; permission & detection logs.	Workflows – Workflow History; Compliance – reporting / logs

Out of scope

These apps do not provide MFA (Art. 21(2)(j)), cryptography/encryption (h), supply-chain security (d), secure development/vulnerability handling (e), network monitoring, business-continuity execution, incident detection/response, or the Article 23 reporting timelines (24h / 72h / one-month final report). They support the documented-governance and access-control layer only. NIS2's measures map closely to ISO/IEC 27001 — build once, evidence both. Guidance only, not legal advice; NIS2 is implemented through national law that varies by member state.