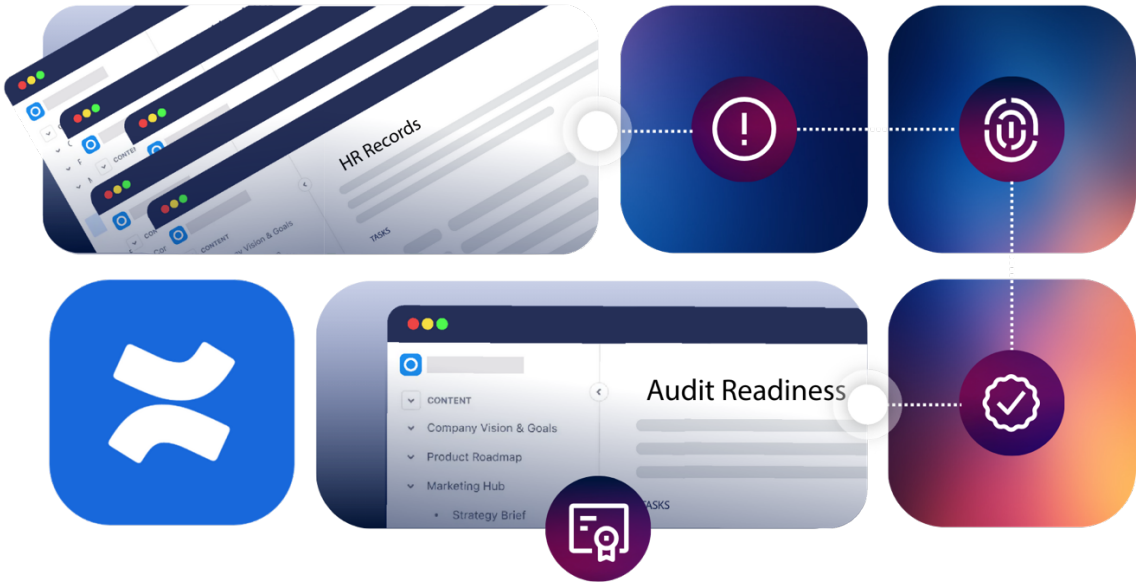
ISO 27001:2022 Evidence Checklist for Confluence

Compliance for Confluence + Workflows for Confluence | AppFox



ISO 27001 cares less about where your policies, SOPs and audit evidence live than whether they are classified, access-controlled, approved, reviewed on a schedule, and backed by an audit trail. This checklist maps the controls you can realistically evidence inside Confluence to the exact tooling (Compliance for Confluence or Workflows for Confluence) that delivers it. References use the current ISO/IEC 27001:2022 structure. An editable Excel tracker version for use as a working template is also available here.

ISO 27001:2022 reference	Requirement (in brief)	Evidence an auditor expects	How to produce it in Confluence (app – feature)
1. Classify information			
A.5.12 Classification of information	Establish and apply a classification scheme based on sensitivity.	Documented scheme; content carries a classification level.	Compliance – Classification Levels (Level Schemes)
A.5.13 Labelling of information	Label information per the scheme.	Visible classification banner on each page.	Compliance – Classification banners
A.5.9 Inventory of information & associated assets	Maintain an inventory of information assets and owners.	Report of classified pages and owners (Confluence portion).	Compliance – Dashboard & reporting
2. Restrict access			
A.5.15 Access control	Restrict access on a need-to-know basis.	Access rules tied to classification; documented approach.	Compliance – Restriction Schemes bound to Levels
A.8.3 Information access restriction	Technically restrict access to information.	Page-level restrictions enforced automatically.	Compliance – Enhanced Page Restrictions
A.8.2 Privileged access rights	Restrict and manage privileged/edit access.	Restricted edit groups; permission report.	Compliance – Restriction Schemes + reporting
A.5.18 Access rights	Provision, review and remove access periodically.	Periodic access-review evidence with permission export.	Compliance – permission reporting & export

ISO 27001:2022 reference	Requirement (in brief)	Evidence an auditor expects	How to produce it in Confluence (app – feature)
3. Detect & prevent exposure			
A.8.12 Data leakage prevention	Apply DLP measures where sensitive info is handled.	Detection results and remediation / automation evidence.	Compliance – Sensitive Data Detection + Automation Rules
4. Control the document lifecycle			
Clause 7.5 Documented information	Approve documents for adequacy; control versions.	Approval records; current/controlled version identified.	Workflows – Approval & Official Version Workflows
A.5.1 Policies for information security	Policies approved by management, published, communicated.	Management-approved, published policy set with sign-off.	Workflows – Approval Workflows (e-signatures) + Publishing Control
A.5.37 Documented operating procedures	SOPs documented, maintained, available to those who need them.	Approved SOPs, access-controlled by role.	Workflows – approval/publishing; Compliance – role restriction
A.5.10 Acceptable use of information	Acceptable-use rules established and acknowledged.	Policy acknowledgement / acceptance records.	Workflows – acceptance workflow; Compliance – banners
5. Keep documents current			
A.5.1 (review) / Clause 10.1 Continual improvement	Review policies and procedures at planned intervals.	Dated review/re-approval records; automatic triggers.	Workflows – Content Expiration / page expiry
6. Build the audit trail			
A.8.15 Logging	Produce, retain and review activity logs.	Workflow history; permission-change & detection logs.	Workflows – Workflow History (export); Compliance – logs/Dashboard
Clause 9.1 Monitoring, measurement, analysis & evaluation	Monitor and evaluate ISMS performance.	Dashboards/reports of control operation over time.	Compliance – Dashboard; Workflows – Search & reporting
A.5.36 Compliance with policies, rules & standards	Demonstrate ongoing conformance.	Exported audit evidence packs.	Workflows – history export; Compliance – report exports
7. Integrate · 8. Legal · 9. Improve			
Clause 9.1 / A.8.16 Monitoring activities	Feed Confluence control data into central monitoring/GRC.	Evidence exported to SIEM/GRC.	Compliance – REST API
A.5.31 Legal, statutory, regulatory & contractual requirements	Identify and meet legal/contractual obligations.	Audit trail of documentation and access control.	Compliance – reporting; Workflows – history
Clause 10.2 Nonconformity & corrective action	Manage nonconformities and corrective actions.	Workflow-tracked corrective actions with history.	Workflows – corrective-action workflows + audit history

Scope note

No tool makes you compliant on its own. These apps cover the information you manage in Confluence; your overarching ISMS, risk assessment, Statement of Applicability, people controls (A.6), and network / endpoint / physical and incident-response controls sit around them. Both apps offer a 30-day free trial on the Atlassian Marketplace. Full guides at docs.appfox.io. © Automation Consultants - an ISO 27001, Cyber Essentials Plus and SOC 2 accredited organisation.