Get Audit-Ready Today

At A9 Consulting Group, we embed continuous security and compliance into your Atlassian workflows—transforming audits from high-cost, reactive events into predictable, manageable habits. Think of us as cost-effective insurance and a good operational discipline that keeps your team always one step ahead of auditors.

Ready to lock down your environment? **Request your 15-Minute Security Discovery Call** and let's turn your next audit into a non-event.

---

1. **Enable and verify audit logging for Jira, Confluence, and Bitbucket**
    - **Problem:** Without centralized, tamper-resistant logs, changes and user actions go untracked—blocking forensic analysis and compliance validation.
    - **A9 Approach:** Configure and validate native audit-log settings across all Atlassian products, ensure retention policies meet requirements, and integrate logs into your SIEM or centralized log store for real-time monitoring.
2. **Review and tighten global permissions; remove unused or overly broad roles**
    - **Problem:** Excessive or stale global permissions create unnecessary attack vectors and make it impossible to enforce least-privilege.
    - **A9 Approach:** Analyze every global permission scheme, identify unused or over-privileged roles, and apply a least-privilege redesign—removing or consolidating roles to minimize your blast radius.
3. **Audit project permission schemes for each project; ensure least-privilege**
    - **Problem:** Inconsistent project-level permissions can expose sensitive issues or workflows to unauthorized users.
    - **A9 Approach:** Enumerate all project schemes, benchmark them against policy, and automate remediation of any deviations—ensuring only required groups and roles retain access.
4. **Identify and deactivate orphaned user accounts and service accounts**

- **Problem:** Dormant or orphaned accounts remain a hidden entry point for attackers once compromised.
- **A9 Approach:** Cross-reference your user directory (AD/Okta) with active Atlassian accounts, flag orphans, and implement automated deprovisioning workflows to remove them promptly.

5. **Validate SSO/SAML configurations and enforce MFA for all administrative users**

    - **Problem:** Weak or misconfigured SSO flows and missing multi-factor authentication allow privilege escalation and account takeover.
    - **A9 Approach:** Perform a thorough SSO/SAML configuration review, tighten assertion and certificate settings, and enforce mandatory MFA policies for every high-privilege account.

6. **Review application API tokens and revoke unused or expired tokens**

    - **Problem:** Forgotten or never-rotated API tokens can be misused to exfiltrate data or pivot laterally.
    - **A9 Approach:** Inventory all active tokens, identify stale or overly scoped credentials, and automate token rotation and revocation processes to eliminate standing secrets.

7. **Confirm encryption-in-transit (TLS) and encryption-at-rest settings are enabled**

    - **Problem:** Lack of end-to-end encryption exposes customer data and configuration details to network-level interception.
    - **A9 Approach:** Audit TLS configurations against industry best practices (ciphers, protocols), verify storage encryption settings, and remediate any gaps to ensure data remains protected at every layer.

8. **Check integrations (webhooks, apps) for minimal required scopes and permissions**

    - **Problem:** Over-privileged integrations turn third-party apps into backdoors for data access or privilege escalation.
    - **A9 Approach:** Catalog every webhook and app integration, evaluate required scopes, and implement a permissions hardening plan—locking down each integration to only the APIs it truly needs.

9. **Ensure custom fields and ScriptRunner/Forge scripts have been peer-reviewed and signed-off**

    - **Problem:** Unauthorized or unvetted custom code can introduce logic flaws, backdoors, or data leaks.

- **A9 Approach:** Establish a peer-review process for all custom fields and scripts, run static analysis on ScriptRunner/Forge code, and enforce a signing-off gate before deployment.

10. **Run vulnerability scan against custom endpoint URLs (REST, SOAP, GraphQL)**

    - **Problem:** Unseen custom endpoints often harbor injection flaws, authentication bypasses, or information disclosure.
    - **A9 Approach:** Execute authenticated and unauthenticated scans against every custom endpoint, report discoveries with risk ratings, and guide your team through prioritized remediation.

11. **Export configuration snapshots and package evidence for auditor review**

    - **Problem:** Manual evidence collection is time-consuming and error-prone, risking missed data during audits.
    - **A9 Approach:** Automate configuration exports (schemas, permission snapshots, policy definitions) into timestamped bundles that map directly to auditor checklists.

12. **Schedule automated compliance reports (weekly/bi-weekly) and distribute to stakeholders**

    - **Problem:** Ad-hoc reporting leaves audit gaps and forces firefighting right before reviews.
    - **A9 Approach:** Build a report-as-code pipeline—generating, distributing, and archiving compliance summaries on your cadence, complete with change diffs and remediation status.

13. **Document change-management processes for configuration updates and permissions changes**

    - **Problem:** Lack of formal documentation leads to unauthorized or untracked changes, undermining audit integrity.
    - **A9 Approach:** Blueprint and document every step of your change-management workflow—capturing approvals, timestamps, and roll-back plans in a centralized register.

14. **Maintain a baseline config file (as code) to detect drift and unauthorized changes**

    - **Problem:** Configuration drift sneaks in misconfigurations over time, eroding security posture.
    - **A9 Approach:** Codify your Atlassian configuration into version-controlled “config-as-

code," implement drift detection, and trigger alerts or automated remediations on any divergence.

15. **Conduct a simulated pentest covering critical workflows and document findings**

    - **Problem:** Without real-world attack simulations, critical workflow vulnerabilities remain undiscovered until exploited.
    - **A9 Approach:** Perform targeted red-team exercises on high-risk workflows, produce a prioritized findings report, and collaborate on mitigation plans to close every identified gap.

Next Step: Let's schedule your discovery call and kick off the pilot—so you can start treating audit readiness as an ongoing advantage, not a last-minute scramble.