MPS 23 – Audits and Reviews

Category: Proof It Works

Tags: audit, review, remote assurance, independent verification, data analytics, operational maturity, ISO19011, ISO27001, continuous improvement, proof

Description: Minimum Performance Standard for Audits and Reviews. Defines the intent, required actions, and guidance for systematically evaluating the effectiveness, compliance, and continual improvement of security management systems and controls. Emphasises the generation of standardised, auditable evidence to support remote, independent assurance and data-driven oversight aligned with international frameworks such as ISO 19011, ISO 27001, and NIST.

Assessment Criteria (Structured)

1. 1.

Requirement: An approved annual audit plan must align with site risk profiles and be signed off by senior leadership.

Evidence: Signed plan document, risk-aligned audit schedules, and CRO/Risk Manager approval logs.

2. 2.

Requirement: Regular planned inspections, reviews, and audits must be conducted and systematically logged.

Evidence: Audit reports, inspection records, and audit log systems with remote access functionality.

3. 3.

Requirement: Internal evaluations must assess control effectiveness, compliance, and be recorded in auditable systems.

Evidence: Internal audit summaries, system compliance checks, and review logs.

4. 4.

Requirement: External audits must be conducted periodically by qualified independent parties based on agreed criteria.

Evidence: External audit contracts, certification records, and completed audit summaries.

5. 5.

Requirement: Audit processes must include automated workflows and data analytics covering at least 80% of defined criteria.

Evidence: Automation system outputs, analytics dashboards, and continuous evaluation logs.

6. 6.

Requirement: A systematic process must exist for logging findings, assigning corrective actions, tracking progress, and verifying closure.

Evidence: CAPA logs, task trackers, and audit improvement closure reports.

7. 7.

Requirement: Security Framework Reviews must evaluate the suitability of policies, systems, and performance trends at planned intervals.

Evidence: Review meeting records, performance dashboards, and improvement plans.

8. 8.

Requirement: Reviews must identify reasons for changes, extent of revisions, resources, accountabilities, and expected benefits.

Evidence: Review outputs, change implementation logs, and stakeholder sign-off forms.

9. 9.

Requirement: Records of audits and reviews must be securely stored and accessible for remote, independent verification.

Evidence: Encrypted storage systems, access logs, and archival policy documents.