

MPS 25 – Remote Assurance

Category: Proof

Tags: remote assurance, monitoring, independent oversight, risk management, compliance, data analytics, incident management, continuous improvement

Description: Minimum Performance Standard for Remote Assurance. Defines the intent, required actions, and guidance for implementing an independent, off-site, objective monitoring function that uses data integration and analytics to ensure effective risk management, loss prevention, compliance, and continual improvement. Aligns with ISO 31000 and ISO 37301 standards for risk and compliance assurance, supporting continuous visibility, verification, and audit readiness.

Assessment Criteria (Structured)

1. 1.

Requirement: A Remote Assurance Policy or Procedure must be approved, documented, and communicated, outlining scope, objectives, roles, and responsibilities.

Evidence: Signed policy document, version history, and distribution records.

2. 2.

Requirement: An independent off-site monitoring capability must be established with documented authority and autonomy.

Evidence: Organisational charts, job descriptions, and governance approvals.

3. 3.

Requirement: Data feeds must be integrated from surveillance, access control, incident management, SCADA/process control, HR/payroll, and procurement systems.

Evidence: Integration diagrams, API logs, and access records.

4. 4.

Requirement: Real-time monitoring systems must support live alerting, automated escalation, and audit trails.

Evidence: Alert logs, escalation rules, and event response summaries.

5. 5.

Requirement: Incident management systems must reflect independent review of logs, footage, reports, and control data.

****Evidence:**** Incident records with third-party review tags and investigation outcomes.

6. 6.

****Requirement:**** Structured dashboards must be used to visualise risk thresholds and key performance indicators.

****Evidence:**** Risk dashboards, heat maps, and threshold breach logs.

7. 7.

****Requirement:**** Reporting and escalation protocols must define notification paths and track closure of findings.

****Evidence:**** Notification records, case closure tracking, and approval signatures.

8. 8.

****Requirement:**** Secure handling protocols must be in place for data storage, access control, and privacy compliance.

****Evidence:**** Data handling procedures, access logs, and encryption verification.

9. 9.

****Requirement:**** Continuous improvement logs must reflect policy revisions, lessons learned, and control enhancements based on assurance insights.

****Evidence:**** CAPA logs, policy update trackers, and audit review notes.