MPS 24 – Security Information Management and Analysis

Category: Proof

Tags: security information management, threat environment, environmental scan, analysis, remote assurance, compliance, human rights, data protection, ISO31000, NIST, proof

Description: Minimum Performance Standard for Security Information Management and Analysis. Defines the intent, required actions, and guidance for building a structured, ethical, and rights-respecting process to collect, analyse, manage, and share security-relevant information. Emphasises professionalism, transparency, and auditability, with robust records to support remote, independent assurance, ongoing threat monitoring, and continuous improvement. Aligns with ISO 31000, ISO 27001, NIST frameworks, and human rights principles (UNGPs, VPSHR).

Assessment Criteria (Structured)

1. 1.

Requirement: An approved Security Information Management Framework must be maintained, aligned with best practices and reviewed annually.

Evidence: Approved framework document and annual review log.

2. 2.

Requirement: An annual documented Business Environmental Scan must analyse internal and external threats.

Evidence: Scan reports, threat maps, and update records.

3. 3.

Requirement: A Structured Information Management Cycle must be implemented with defined planning, collection, analysis, and dissemination processes.

Evidence: Cycle documentation, SOPs, and communication logs.

4. 4.

Requirement: Internal roles and responsibilities must be clearly defined and comply with ethics, privacy, and human rights standards.

Evidence: Role descriptions, assignment logs, and training records.

5. 5.

Requirement: Records must be standardised, auditable, searchable, and support remote assurance.

Evidence: Metadata logs, access controls, and archive policies.

6. 6.

Requirement: Engagement with government, law enforcement, and peers must be formalised and documented.

Evidence: Meeting logs, contact registers, and partner engagement records.

7. 7.

Requirement: Regular meeting schedules must exist with formal briefings to senior management.

Evidence: Meeting agendas, notes, and briefing summaries.

8. 8.

Requirement: Internal authority limits must be clearly defined for information management personnel.

Evidence: Policy excerpts and role restriction logs.

9. 9.

Requirement: Security incident reports must be continuously analysed to detect patterns and vulnerabilities.

Evidence: Incident logs, analytical summaries, and anomaly detection outputs.

10. 10.

Requirement: Cross-referencing must be conducted with access control, CCTV, seal logs, and supply chain data.

Evidence: Cross-reference reports and data linkage examples.

11. 11.

Requirement: Professional analysis standards must be applied including methodology, forecasting, and evidence-based reporting.

Evidence: Analysis templates, testing protocols, and final reports.

12. 12.

Requirement: Regular training must be provided on analysis techniques, human rights, and data protection.

Evidence: Training logs, course content, and attendance certificates.

13. 13.

Requirement: Secure data management practices must include encryption, access control, and defined retention/disposal schedules.

Evidence: Encryption logs, access records, and disposal audit trails.

14. 14.

Requirement: Outputs must be timely, actionable, and shared with relevant stakeholders.

Evidence: Threat bulletins, risk advisories, and distribution logs.

15. 15.

Requirement: Analysis results must feed into continuous improvement processes and maturity planning.

Evidence: Policy updates, planning notes, and roadmap alignment evidence.