

MPS 5 – Legal and Regulatory Requirements

****Category:**** Leadership and Governance

****Tags:**** legal compliance, regulatory requirements, governance, policy, audit readiness, security assurance

****Description:**** Minimum Performance Standard for Legal and Regulatory Compliance. Defines the intent, required actions, and guidance to ensure the organisation meets all applicable laws, regulations, standards, and contractual obligations. Emphasises establishing clear governance structures, responsibilities, and processes for monitoring and maintaining compliance within security operations and across the business.

Assessment Criteria (Structured)

1. 1.

****Requirement:**** An approved Legal and Regulatory Compliance Policy or Framework must be in place, aligned with ISO 37301 principles.

****Evidence:**** Policy document with defined scope, governance structure, and responsibilities.

2. 2.

****Requirement:**** A Compliance Register must be maintained, covering all laws, regulations, standards, and contracts with assigned owners.

****Evidence:**** Register documents, owner assignments, review schedules, and update logs.

3. 3.

****Requirement:**** Processes must exist to identify, assess, and manage new or changing legal and regulatory obligations.

****Evidence:**** Records of legal scans, impact assessments, and stakeholder reviews.

4. 4.

****Requirement:**** The Compliance Register must be reviewed and updated regularly, with change logs and formal approvals.

****Evidence:**** Version-controlled documents with audit trails of updates and sign-offs.

5. 5.

****Requirement:**** Roles and responsibilities for compliance must be documented using job descriptions and/or RACI matrices.

****Evidence:**** HR files or governance documentation assigning compliance-related duties.

6. 6.

****Requirement:**** All relevant personnel must be trained on applicable legal and regulatory requirements and ethical responsibilities.

****Evidence:**** Training records, attendance logs, and evaluation reports.

7. 7.

****Requirement:**** A Compliance Monitoring Program must be implemented, including audits, self-assessments, and third-party reviews.

****Evidence:**** Audit schedules, reports, and corrective action trackers.

8. 8.

****Requirement:**** Senior management must review compliance performance and risks regularly through formal governance channels.

****Evidence:**** Meeting minutes, board reports, and documented leadership responses.

9. 9.

****Requirement:**** Compliance expectations must be communicated to internal teams and relevant external stakeholders.

****Evidence:**** Internal communications, supplier agreements, and training briefings.

10. 10.

****Requirement:**** Incident reporting and investigation procedures must address potential legal or regulatory breaches.

****Evidence:**** Incident logs, investigation reports, and corrective action records.

11. 11.

****Requirement:**** Records must be retained to demonstrate compliance with legal and regulatory requirements.

****Evidence:**** Licenses, certifications, submissions to regulators, and audit confirmations.