MPS 4 – Risk Management

Category: Leadership and Governance

Tags: risk management, security, ISO 31000, NIST, governance, adversarial threats, controls, ERM, ORM

Description: Minimum Performance Standard for Risk Management. Defines the intent, required actions, and guidance to ensure the organisation adopts a consistent, structured approach to identifying, assessing, and controlling risks. Emphasises alignment with international standards such as ISO 31000 and NIST, with specific focus on adversarial threats, security risk management, and operational integration.

Assessment Criteria (Structured)

1. 1.

Requirement: The organisation must maintain an approved Risk Management Policy and Framework aligned with ISO 31000.

Evidence: Policy and framework documents with approval signatures and ISO 31000 references.

2. 2.

Requirement: The Enterprise Risk Management (ERM) Policy must define the risk process and assign roles to Board, Committees, and staff.

Evidence: ERM Policy outlining responsibilities, decision levels, and methodology.

3. 3.

Requirement: Security risk assessments must incorporate NIST guidance for adversarial threat modelling and response planning.

Evidence: Completed SRAs using NIST templates or threat analysis methodologies.

4. 4.

Requirement: All risk registers must follow a standardised format including impact, likelihood, control effectiveness, and response planning.

Evidence: Risk registers with consistent layout and scoring model.

5. 5.

Requirement: Critical controls for high and very high risks must be clearly defined, resourced, and regularly tested.

Evidence: Control plans, resource allocation, and control testing logs.

6. 6.

Requirement: Risk registers must be reviewed and updated at least annually or upon material change for high-risk items.

Evidence: Dated register updates, change logs, and review meeting records.

7. 7.

Requirement: Risk and incident systems must be integrated to ensure complete risk identification and resolution tracking.

Evidence: Links or data integrations between incident and risk platforms.

8. 8.

Requirement: Staff must be trained in applying risk assessment tools at task and incident level.

Evidence: Training attendance records, course content, and evaluation summaries.

9. 9.

Requirement: Security policies and procedures must align directly with the risk management strategy.

Evidence: Policy mapping tables, SOP references within risk framework documents.