MPS 20 – Resilience and Recovery

Category: Protection

Tags: resilience, business continuity, risk management, incident response, recovery planning, stakeholder engagement, protection

Description: Minimum Performance Standard for Resilience and Recovery. Defines the intent, required actions, and guidance for ensuring the organisation has structured, risk-informed plans and capabilities to identify, mitigate, control, and recover from incidents that disrupt operations. Emphasises integration with enterprise risk management, comprehensive business continuity planning (BCP), stakeholder coordination, and continuous improvement to build resilience.

Assessment Criteria (Structured)

1. 1.

Requirement: Departmental Business Continuity Plans (BCPs) must align with the BCM policy and cover six continuity pillars: functions, skillsets, equipment, documentation, suppliers, and IT systems.

Evidence: Approved BCPs mapped to continuity pillars with periodic reviews.

2. 2.

Requirement: Departmental BCP risks must be recorded in the Governance, Risk, and Compliance system and align with the enterprise risk register.

Evidence: Risk logs showing integration across levels and evidence of cross-functional consistency.

3. 3.

Requirement: Risk identification must follow structured, documented methodologies and avoid isolated assessments.

Evidence: Methodology documentation and sample risk identification reports.

4. 4.

Requirement: Major risks must be clearly defined in formal risk management procedures.

Evidence: Defined risk entries and supporting analysis records.

5. 5.

Requirement: Trigger Action Response Plans (TARPs) must exist for each major risk and include predefined thresholds and actions.

Evidence: Approved TARPs with response timelines, escalation paths, and trigger thresholds.

6. 6.

Requirement: TARPs must define critical spares, stakeholder roles, immediate actions, training requirements, budgets, and lessons learned procedures.

Evidence: Full TARP documentation with stakeholder contact lists, training calendars, and resourcing logs.

7. 7.

Requirement: Operational planning must address responses to defined events including natural disasters, cybercrime, civil emergencies, pandemics, and evacuation scenarios.

Evidence: Response playbooks and scenario-specific protocols.

8. 8.

Requirement: Employees must demonstrate awareness and incorporation of resilience planning into their functional areas.

Evidence: Training logs, awareness campaigns, and team-level procedures.

9. 9.

Requirement: Procurement must maintain verified, management-approved lists of critical spares.

Evidence: Signed spare parts lists with integrity checks and procurement validation.