MPS 14 – Continuous Improvement

Category: People and Culture

Tags: continuous improvement, incident management, root cause analysis, corrective actions, risk management, governance, ISO 9001, ISO 31000, ISO 45001

Description: Minimum Performance Standard for Continuous Improvement. Defines the intent, required actions, and guidance for establishing systematic approaches to learning from incidents, non-conformities, stakeholder feedback, audits, and management reviews to strengthen security and risk management practices over time. Supports proactive identification of weaknesses, structured investigations, formal corrective and preventive actions, and organisational learning aligned with international standards including ISO 9001, ISO 31000, and ISO 45001.

Assessment Criteria (Structured)

1. 1.

Requirement: A documented Continuous Improvement Policy or Framework must define objectives, scope, and responsibilities.

Evidence: Approved policy document outlining intent, principles, and oversight structure.

2. 2.

Requirement: An approved Incident Management System must support reporting, recording, and classifying incidents and near misses.

Evidence: Incident system logs, procedures, and classification forms.

3. 3.

Requirement: Incident escalation procedures must define roles, responsibilities, and response timelines.

Evidence: Escalation matrices, response flowcharts, and role descriptions.

4. 4.

Requirement: Incidents must be classified using risk-based systems aligned with ISO 31000 principles.

Evidence: Classification tools, consequence/likelihood matrices, and applied samples.

5. 5.

Requirement: Accountable persons must be assigned to conduct and oversee incident investigations.

Evidence: Investigation delegation records and accountability documents.

6. 6.

Requirement: Personnel involved in investigations must meet defined competency requirements and receive appropriate training.

Evidence: Training records, competency checklists, and certifications.

7. 7.

Requirement: Structured Root Cause Analysis (RCA) methods must be applied consistently across incidents.

Evidence: RCA reports, cause mapping templates, and case study logs.

8. 8.

Requirement: A formal CAPA (Corrective and Preventive Action) process must guide action documentation, approval, and verification.

Evidence: CAPA forms, action trackers, and approval logs.

9. 9.

Requirement: Corrective actions must be tracked to verify closure and effectiveness.

Evidence: Follow-up reports, verification notes, and closure confirmations.

10. 10.

Requirement: Regular management reviews must evaluate incident trends and the effectiveness of improvement initiatives.

Evidence: Meeting records, dashboards, and improvement action summaries.

11. 11.

Requirement: Lessons learned must be shared organisation-wide through formal procedures.

Evidence: Shared reports, email summaries, team debriefs, or internal bulletins.

12. 12.

Requirement: External reporting procedures must be in place to meet legal or regulatory disclosure obligations.

Evidence: Submission logs, regulatory communications, and reporting procedures.

13. 13.

Requirement: Periodic audits or reviews must verify system integrity and drive enhancement opportunities.

Evidence: Audit checklists, findings reports, and improvement action logs.

14. 14.

Requirement: Stakeholder engagement processes must capture feedback on controls and incident handling.

Evidence: Stakeholder feedback forms, engagement meeting minutes, and action logs.

15. 15.

Requirement: Continuous improvement requirements must be integrated into broader risk management frameworks.

Evidence: Evidence of alignment with ISO 9001, ISO 31000, and ISO 45001 across integrated systems.