MPS 7 – Process Control and Operational Failure Management

Category: Process Integrity

Tags: process control, incident management, root cause analysis, change control, bypass detection, sabotage prevention, risk mitigation, operational integrity, audit trail

Description: Minimum Performance Standard for Process Control and Operational Failure Management. Defines the intent, required actions, and guidance to ensure critical operational processes are designed, controlled, and continuously monitored to prevent failures, deviations, or bypasses that may impact safety, security, quality, or performance. This standard supports risk-based control design, structured workflows, incident reporting, change management, and root cause analysis.

Assessment Criteria (Structured)

1. 1.

Requirement: Process flows or SOPs must be documented, outlining control points, risk criteria, and responsibilities.

Evidence: Approved SOPs or visual maps with roles, steps, and embedded controls.

2. 2.

Requirement: Operational environments must be maintained to support effective execution and process visibility.

Evidence: Layout plans, inspection reports, and environmental condition logs.

3. 3.

Requirement: Security and risk controls must be embedded in procedures for high-risk operations or overrides.

Evidence: Procedures showing embedded checkpoints, access control layers, and override restrictions.

4. 4.

Requirement: All operational changes must follow formal change management protocols with risk justifications.

Evidence: Change request logs, risk assessments, and approval records.

5. 5.

Requirement: Known bypasses or overrides must be tracked and prioritized in a live register with mitigation plans.

Evidence: Bypass register, interim fix notes, and resolution timelines.

6. 6.

Requirement: Personnel must be educated on process manipulation risks and proper change protocols.

Evidence: Training records, job aids, and signed acknowledgements.

7. 7.

Requirement: Operational systems must be monitored for abnormal conditions or process deviations.

Evidence: SCADA data, variance reports, alert thresholds, and daily monitoring logs.

8. 8.

Requirement: Sabotage or manipulation patterns must be identified using behavioral and cross-system analytics.

Evidence: Surveillance records, anomaly reports, and correlation dashboards.

9. 9.

Requirement: Infrastructure risk reviews must be conducted and documented regularly.

Evidence: Power, software, and mechanical risk assessments with inspection results.

10. 10.

Requirement: Engineering and risk documentation must be maintained and updated.

Evidence: Design documents, safety audits, and external compliance reviews.

11. 11.

Requirement: Weekly risk reviews must be conducted on high-value or critical processes.

Evidence: Meeting logs, trend reports, and proactive risk tracking tools.

12. 12.

Requirement: Operators must be trained on control limits, response actions, and intervention boundaries.

Evidence: Training completion certificates, session feedback, and test results.

13. 13.

Requirement: Behavioral compliance must be monitored in sensitive zones and escalated as needed.

Evidence: Incident reports, access logs, PPE compliance checks, and disciplinary actions.

14. 14.

Requirement: All significant process incidents must trigger RCA and CAPA tracking to resolution.

Evidence: Root cause reports, CAPA logs, lessons learned, and closure confirmations.