MPS 2 – Chain of Custody and Security Control Committee

Category: Leadership and Governance

Tags: chain of custody, governance, accountability, security control committee, security management, compliance

Description: Minimum Performance Standard for Chain of Custody and Security Control Committee. Defines intent, required actions, and guidance to ensure clear accountability for the custody of high-value materials or assets, with robust governance through an operationally embedded Security Control Committee, maintaining integrity from source to destination.

Assessment Criteria (Structured)

1.
Requirement: A documented Chain of Custody Matrix must be established, assigning named accountability across all operational stages.

Evidence: Approved Chain of Custody Matrix with named owners, version control, and review records.

2.
Requirement: The Chain of Custody Matrix must be reviewed and updated annually or after key personnel/process changes.

Evidence: Matrix showing annual reviews or updates tied to personnel or process change events.

3.
Requirement: The Chain of Custody Matrix must be displayed in an accessible format, with controls listed per segment.

Evidence: Posted matrix with readable segmentation and clear accountability markers.

4.
Requirement: A Security Control Committee must be established and chaired by the senior operational executive or designate.

Evidence: Formal committee appointment records, chair assignment, and org structure.

5.
Requirement: A Security Control Committee Charter must be signed by senior leadership, defining scope, responsibilities, and meeting cadence.

Evidence: Approved and signed charter with documented scope, roles, and meeting intervals.

6.
Requirement: A current RACI chart must be maintained, aligned to the Security Control Standard, and signed off by senior management.

Evidence: Dated RACI chart signed by key stakeholders, showing coverage across functions.

7.
Requirement: Security Control Committee meetings must be held at least quarterly, with actions, accountability, and attendance recorded.

Evidence: Meeting minutes with decisions, attendees, and follow-ups.

8.
Requirement: High-risk areas must have joint procedures approved by the Security Control Committee and integrated into SOPs.

Evidence: Joint SOPs with approval stamps and control integration references.

9.
Requirement: Root cause analyses must be conducted for significant security incidents under committee oversight.

Evidence: Analysis reports, incident logs, and committee-reviewed action plans.

10.
Requirement: Leadership reviews must be held to assess human factors in high-risk areas including training, recruitment, and spans of control.

Evidence: Reports addressing performance management, HR risk reviews, and governance summaries.

11.
Requirement: Security performance metrics must be tracked and reviewed in committee meetings.

Evidence: Dashboards, trend graphs, and committee discussion notes.

12.
Requirement: Security design changes must be reviewed and approved by the Security Control Committee.

Evidence: Design approval documents and change review notes with committee references.

13.
Requirement: A dual-tier Security Control Committee structure must be implemented where appropriate.

Evidence: Documentation showing distinct layers of strategic vs operational oversight.

14.
Requirement: Committee role assignments must reflect cross-functional representation, including Risk, Security, and Operations.

Evidence: Committee composition records showing participation from key departments.