MPS 3 – Separation of Duties

Category: Leadership and Governance

Tags: separation of duties, governance, accountability, risk management, security assurance

Description: Minimum Performance Standard for Separation of Duties. Defines the intent, required actions, and guidance to reduce risks of error, fraud, collusion, and security breaches by structuring roles, responsibilities, and reporting lines to ensure appropriate checks and balances across security operations and organisational functions.

Assessment Criteria (Structured)

1.
Requirement: A Separation of Duties Policy must be approved and must define incompatible functions, responsibilities, and boundaries.

Evidence: Approved policy document outlining prohibited role combinations and assigned responsibilities.

2.
Requirement: All critical roles must have documented job descriptions and be reflected in organisational charts with clear separation of duties.

Evidence: Role descriptions and charts showing assignment and segregation of duties.

3.
Requirement: Security leadership must have independent reporting lines to senior executives or governance committees.

Evidence: Org charts and reporting line documentation showing direct executive access.

4.
Requirement: Security management must conduct regular briefings (at least monthly) with senior executives to report on risks, performance, and strategic needs.

Evidence: Meeting records, agendas, and summary reports from security briefings.

5.
Requirement: Security personnel must formally declare any conflicts of interest and mitigation measures must be in place.

Evidence: Signed declarations, review records, and mitigation plan documentation.

6.
Requirement: Security oversight of operational functions must be documented and include escalation paths for non-compliance or risks.

Evidence: Escalation charts, issue logs, and governance process records.

7.
Requirement: All relevant personnel must receive training on separation-of-duties expectations and role boundaries.

Evidence: Training records, attendance sheets, and training content summaries.

8.
Requirement: Security performance must be measured using KPIs and reported to executive or governance bodies.

Evidence: KPI dashboards, trend reports, and governance meeting references.

9.
Requirement: Security procedures, post orders, and SOPs must be maintained, version-controlled, and accessible.

Evidence: Procedure documents with version history and last review dates.

10.
Requirement: Security Managers with other duties must have clear workload allocation ensuring priority for security responsibilities.

Evidence: Workload analysis documents, time allocation plan