MANAGEMENT REVIEW PROCEDURE

INLINE WITH ISO 27001:2022 & SOC 2

Prepared By :

MINISTRY OF MOS SECURITY

Document Name	**Management Review Procedure**
Classification	**Internal Use Only**

Document Management Information

Document Title:	Management Review Procedure
Document Number:	ORGANISATION-MNM-REV-PRO
Document Classification:	Internal Use Only
Document Status:	Approved

Issue Details

Release Date	DD-MM-YYYY

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	DD-MM-YYYY	<Provide details of changes made on policy here>	<Provide name of Approver here>

Document Contact Details

Role	Name	Designation
Author	<Provide name of author here>	<Provide designation of author here>
Reviewer/ Custodian	<Provide name of reviewer here>	<Provide designation of reviewer here>
Owner	<Provide name of owner here>	<Provide designation of owner here>

Distribution List

Name
Need Based Circulation Only

Document Name	Management Review Procedure
Classification	Internal Use Only

CONTENTS

Document Name	Management Review Procedure
Classification	Internal Use Only

1. PURPOSE

The purpose of this Management Review Procedure is to establish a structured and systematic process for senior management to regularly review the effectiveness, adequacy, and continual improvement of [ORG NAME]'s **Information Security Management System (ISMS)** and related internal controls supporting **SOC 2 Type 2** compliance.

This procedure ensures that:

- The ISMS remains aligned with [ORG NAME]'s business strategy, risk appetite, and external obligations.
- Management is informed of the current state of security, compliance, and risk.
- Key performance indicators (KPIs), audit results, incidents, and improvement opportunities are reviewed and addressed.
- Resources and responsibilities are allocated to maintain and enhance the ISMS and SOC 2 control environment.
- The organization meets its obligations under **ISO/IEC 27001:2022 Clause 9.3 (Management Review)**, **SOC 2 Trust Services Criteria (Governance & Monitoring)**, and other applicable standards.

This procedure promotes accountability at the leadership level and supports continual improvement by translating review outcomes into actionable plans and decisions.

2. SCOPE

2.1 Organizational Scope

- Includes all departments, business units, teams, and locations within [ORG NAME] that handle, process, or support information security and compliance activities.
- Applies to all processes, systems, services, and third-party engagements that fall within the ISMS and/or SOC 2 reporting boundary.

2.2 Personnel Scope

- Senior management and executive leadership responsible for strategic decisions.
- Functional and departmental heads responsible for operational and security controls.
- ISMS Manager / CISO, Data Protection Officer (if applicable), Internal Audit, and Compliance teams.
- Any other key stakeholders contributing to or impacted by ISMS and SOC 2 objectives.

2.3 Temporal Scope

- Regular, scheduled management reviews (at least annually, preferably quarterly or bi-annually).
- Ad-hoc reviews triggered by significant events, such as:
    - Major security incidents or breaches.
    - Substantial changes to legal, regulatory, or contractual requirements.
    - Findings from internal or external audits.
    - Material changes in business context, risk profile, or technology.

This procedure does not replace operational meetings, incident response meetings, or tactical project reviews; it specifically focuses on strategic, policy-level evaluation and decision-making regarding the ISMS and SOC 2 controls.

3. TERMS AND DEFINITIONS

Term	Definition
Management Review	A formal, documented evaluation by senior management of the ISMS and/or SOC 2 control environment to assess effectiveness, alignment, and opportunities for improvement.
ISMS (Information Security Management System)	A set of policies, processes, and controls designed to systematically manage information security risks and protect information assets.
SOC 2 Type 2	A report attesting to the design and operating effectiveness of controls over a defined period, based on the AICPA's Trust Services Criteria.
KPI (Key Performance Indicator)	A measurable value that demonstrates how effectively security and compliance objectives are being achieved.
Nonconformity	A failure to meet a requirement of the ISMS, SOC 2 controls, or applicable policies and standards.
Corrective Action	Steps taken to eliminate the cause of a detected nonconformity to prevent recurrence.
Risk Assessment	The process of identifying, analyzing, and evaluating risks to the confidentiality, integrity, and availability of information.
Audit Findings	Observations, nonconformities, or recommendations identified during internal or external audits.

Term	Definition
Continual Improvement	The ongoing effort to enhance the ISMS and internal controls to achieve higher levels of effectiveness and maturity.

4. ROLES AND RESPONSIBILITIES

Term	Definition
Executive Management / Board of Directors	- Provide strategic direction and oversight of ISMS and SOC 2 controls. - Approve resources and budgets for continual improvement. - Review and endorse outcomes of management reviews.
CISO / ISMS Manager	- Organize and facilitate management review meetings. - Prepare and present inputs such as KPIs, risk status, and incident reports. - Document meeting minutes and track action items.
Department Heads / Business Unit Leaders	- Provide updates on the performance and issues of ISMS and SOC 2 controls in their respective areas. - Ensure follow-up on assigned corrective actions.
Internal Audit / Compliance Team	- Present internal and external audit findings, observations, and recommendations. - Validate closure of previous action items and verify compliance.
Risk Owners	- Report on the status of risks under their responsibility. - Propose adjustments to risk treatment plans as needed.
Data Protection Officer (if applicable)	- Report on privacy-related risks, compliance with data protection laws, and incidents affecting personal data.
IT / Security Operations	- Report on system performance, incident response activities, and monitoring metrics. - Highlight technical improvements or challenges.
Meeting Chairperson (designated)	- Lead the meeting to ensure the agenda is followed and all required inputs and decisions are documented.

5. FREQUENCY AND SCHEDULING

Regular and timely management reviews are essential to ensure that the ISMS and SOC 2 control environment remain effective, relevant, and aligned with [ORG NAME]'s business objectives and obligations.

5.1 Regular Reviews

- Formal **management review meetings shall be conducted at least once per year** as required by ISO/IEC 27001:2022 clause 9.3.
- [ORG NAME] recommends conducting reviews **quarterly or bi-annually** to enhance responsiveness to risks and changes.

5.2 Ad Hoc Reviews

Additional (unscheduled) reviews may be initiated in response to:

- Major security incidents, breaches, or near-misses.
- Significant changes to the organization's structure, strategy, or technology landscape.
- Introduction of new regulatory or contractual requirements.
- Findings from external audits, inspections, or significant internal audit observations.

5.3 Scheduling

- The ISMS Manager / CISO is responsible for **preparing and circulating an annual review calendar**, including proposed dates and agendas.
- Invitations are sent to all required participants at least **two weeks prior to the meeting**.
- The meeting date should allow sufficient time for preparation, data collection, and stakeholder input.

5.4 Attendance

- All designated participants (see Section 4) must attend or send an authorized delegate.
- Attendance and quorum requirements should be recorded and met to validate the meeting outcomes.

6. INPUTS TO THE MANAGEMENT REVIEW

Management reviews shall be based on a comprehensive set of inputs that provide a clear picture of the ISMS and SOC 2 control environment performance, effectiveness, and opportunities for improvement.

The **CISO / ISMS Manager**, with support from other stakeholders, is responsible for collecting, analysing, and presenting these inputs before the meeting.

6.1 Mandatory Inputs

At a minimum, the following inputs shall be included:

Input Area	Examples of Data & Reports
Status of previous actions	Progress on actions decided in previous management reviews, including closure of open items.
Changes in internal and external issues	Changes in business context, stakeholder expectations, regulations, technology, or threat landscape.
Risk status	Results of risk assessment and effectiveness of risk treatment plans; residual risk levels.
Security & compliance objectives	Progress against ISMS objectives, KPIs, SOC 2 commitments, and improvement targets.
Audit findings	Results of internal audits, external audits (e.g., ISO, SOC 2), and corrective/preventive actions.
Incident & breach reports	Security incidents, privacy breaches, near misses, and lessons learned since the last review.
Feedback from interested parties	Complaints, feedback from clients, regulators, staff, or third parties.
Monitoring & measurement results	Metrics on control effectiveness, system performance, and policy compliance.
Opportunities for improvement	Suggestions from staff, auditors, or external benchmarks to enhance ISMS and SOC 2 controls.
Resource adequacy	Assessment of budget, staffing, skills, and technology to maintain and improve controls.
Significant changes	Major organizational, infrastructural, or legal changes impacting the ISMS/SOC 2 environment.

These inputs ensure that management decisions are informed by data-driven insights and aligned with the organization's risk appetite and strategic goals.

7. OUTPUTS OF THE MANAGEMENT REVIEW

The outputs of the management review document the decisions and actions required to improve the effectiveness, suitability, and alignment of the ISMS and SOC 2 control environment with [ORG NAME]'s business objectives and obligations.

These outputs ensure that identified issues are addressed, improvements are initiated, and responsibilities are clearly assigned.

7.1 Required Outputs

Management reviews must result in clear decisions and documented actions related to the following areas:

Output Area	Examples of Actions / Decisions
Improvement of ISMS & SOC 2 controls	Approve initiatives to strengthen policies, processes, or technologies.
Adjustment of risk treatment plans	Revise risk mitigation strategies or residual risk acceptance based on updated assessments.
Resource allocation	Approve or request additional budget, staff, tools, or training where required.
Revision of objectives & KPIs	Update or redefine ISMS and SOC 2 objectives to reflect changes in context or priorities.
Corrective & preventive actions	Assign responsibilities and deadlines to address identified nonconformities, incidents, or audit findings.
Policy or documentation updates	Direct updates to policies, procedures, or records to reflect changes or improvements.
Approval of exceptions or deviations	Approve temporary exceptions to controls, with documented justification and review plan.
Direction for continual improvement	Endorse proposals for ongoing enhancement of ISMS maturity and SOC 2 readiness.

7.2 Action Tracking

- All decisions and actions shall be recorded in the meeting minutes and assigned to specific owners with due dates.

- Progress on action items will be reviewed at subsequent management review meetings.
- Unresolved or overdue actions will be escalated to executive leadership as needed.

8. DOCUMENTATION AND RECORDS

To demonstrate compliance, facilitate audits, and support continual improvement, all management review activities must be properly documented and securely retained.

8.1 Required Documents

The following documents must be prepared and maintained for each management review:

Document	Description
Agenda	Outline of topics to be discussed, aligned with the inputs defined in Section 6.
Attendee List & Sign-in Sheet	Record of participants present (or delegated representatives), including names, roles, and signatures (if applicable).
Presentation Materials	Data, charts, KPIs, risk assessments, and other inputs presented during the meeting
Meeting Minutes	Detailed record of discussions, decisions, and rationales for each topic.
Action Item Log	Table of decisions, assigned owners, deadlines, and status tracking for all outputs
Supporting Evidence	Relevant reports, audit findings, incident summaries, and stakeholder feedback documents.

8.2 Record Retention

- Management review records must be retained for a minimum of **3 years** (or longer if required by contractual, legal, or audit obligations).
- Records shall be stored securely, with access limited to authorized personnel.
- Electronic records should be version-controlled and backed up per [ORG NAME]'s retention and backup policies.

8.3 Auditability

- All documentation must be made available upon request to:
    - Internal and external auditors.
    - Certification or attestation assessors (e.g., ISO 27001, SOC 2 auditors).
    - Regulatory authorities (if applicable).
- Records must demonstrate evidence of management engagement, informed decisions, and follow-through on action items.

9. FOLLOW-UP AND MONITORING

Follow-up and monitoring are critical to ensuring that the decisions, actions, and improvements identified during the management review are effectively implemented, tracked to completion, and contribute to the continual improvement of the ISMS and SOC 2 control environment. This process reinforces accountability, transparency, and progress against organizational objectives.

9.1 Action Item Documentation and Assignment

- Every decision or action point from the management review must be logged in a dedicated **Action Item Register** maintained by the ISMS Manager or designated facilitator.
- Each action item entry shall include at minimum:
    - Unique Action Item ID/reference number.
    - Description of the action/decision.
    - Context or reason for the action (e.g., audit finding, KPI gap, resource need).
    - Owner(s) responsible for execution.
    - Target completion date.
    - Priority level (High, Medium, Low).
    - Required resources or dependencies.

9.2 Tracking and Reporting

- The ISMS Manager shall:
    - Monitor progress against each action item through periodic check-ins with owners.

  - Update the register to reflect current status: Open, In Progress, Completed, Overdue, or Escalated.
  - Identify and document any risks, dependencies, or blockers that could affect timely completion.
- A **status dashboard or summary report** of action items is prepared for:
  - Quarterly leadership meetings.
  - Subsequent management review sessions.
  - Internal or external audits upon request.

9.3 Verification and Validation

- Once an owner reports an action item as complete, the ISMS Manager or designated verifier must:
  - Review evidence of completion (e.g., updated policy, implemented control, training records).
  - Confirm that the intended objective or risk mitigation outcome has been achieved.
  - Mark the action item as Closed only after validation.

9.4 Escalation Procedure

- Overdue or stalled actions must be flagged to the next level of management, based on impact and priority.
- Escalation paths:
  - Owner's line manager → Department Head → CISO → Executive Leadership
- Reassessment of overdue actions may result in reprioritization, resource reallocation, or revised timelines.

9.5 Continual Improvement and Feedback Loop

- Lessons learned during the implementation of action items are recorded and presented in the next management review.
- Suggestions for process optimization, systemic improvements, or preventive measures are extracted and, where appropriate:
  - Integrated into ISMS policies or procedures.
  - Added as new initiatives or objectives for the next cycle.
- Metrics on action item trends (e.g., % completed on time, number of escalations, recurring themes) are analyzed to improve effectiveness.

9.6 Record Retention

- All action item records, including supporting evidence and closure verification, must be retained for a minimum of **3 years**, or longer if required by contractual, legal, or regulatory obligations.

10. POLICY COMPLIANCE AND ENFORCEMENT

All participants in the management review process — including executives, department heads, risk owners, and support staff — are required to adhere to this procedure to ensure effective oversight and continual improvement of the ISMS and SOC 2 control environment.

10.1 Compliance Monitoring

- The CISO/ISMS Manager and Internal Audit/Compliance Team are responsible for monitoring adherence to this procedure.
- Compliance is verified through:
    - Reviews of management review agendas, minutes, and action item logs.
    - Attendance records and documented evidence of decisions.
    - Validation that decisions and actions from previous reviews have been implemented and closed properly.

10.2 Examples of Non-Compliance

Non-compliance may include, but is not limited to:

- Failure to attend scheduled management reviews without appropriate delegation.
- Inadequate preparation or failure to submit required inputs for the review.
- Neglecting to implement or follow up on assigned action items.
- Failure to record or retain evidence of decisions and actions.
- Obstructing or disregarding agreed timelines or escalation protocols.

10.3 Consequences of Non-Compliance

Violations of this procedure may result in corrective or disciplinary actions, depending on the severity and impact of the breach. Possible consequences include:

- Formal warning or retraining.
- Reassignment or revocation of responsibilities.
- Escalation to HR and/or executive leadership.
- Impact on performance evaluations for recurring or significant failures.

- For contractors or vendors: penalties, contract termination, or legal action if applicable.

10.4 Enforcement Authority

The following roles are authorized to enforce this procedure and determine appropriate corrective actions:

- **CISO / ISMS Manager:** Ensures procedural adherence and leads investigations into violations.
- **Executive Management:** Provides final approval of corrective actions for serious or recurring breaches.
- **Internal Audit / Compliance Team:** Reviews compliance as part of regular audits and recommends improvements.

10.5 Continual Improvement

- Any observations of barriers to compliance, procedural gaps, or suggestions for improving participation and effectiveness of the management review process should be communicated to the ISMS Manager for consideration during the next policy review.

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO