INTERNAL AUDIT PROCEDURE

INLINE WITH ISO 27001:2022 & SOC 2

PREPARED BY :

Document Name	**Internal Audit Procedure**
Classification	**Internal Use Only**

Document Management Information

Document Title:	Internal Audit Procedure
Document Number:	ORGANISATION-INT-AUD-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 procedure 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	Internal Audit Procedure
Classification	Internal Use Only

CONTENTS

Document Name	Internal Audit Procedure
Classification	Internal Use Only

1. PURPOSE

The purpose of this Internal Audit Procedure is to establish a structured and risk-based approach for conducting internal audits of the Information Security Management System (ISMS) and associated operational, technical, and compliance controls.

This procedure is designed to:

- Verify the effectiveness of controls implemented as part of [ORG NAME]'s ISMS and SOC 2 Type 2 compliance programs.
- Ensure ongoing conformity with the requirements of **ISO/IEC 27001:2022**, especially Clause **9.2: Internal Audit**, and the **Trust Services Criteria** for **Security, Availability, Confidentiality, Processing Integrity, and Privacy** under SOC 2.
- Identify nonconformities, control weaknesses, and improvement opportunities before external audits or regulatory inspections.
- Provide senior management and the ISMS Steering Committee with objective assurance regarding the performance and maturity of the security program.

By implementing this procedure, [ORG NAME] ensures that its internal audits are conducted systematically, impartially, and effectively — supporting continual improvement of its information security and compliance posture.

2. SCOPE

This procedure applies to all internal audits conducted to assess the adequacy, effectiveness, and compliance of [ORG NAME]'s:

- **Information Security Management System (ISMS)** as per the requirements of ISO/IEC 27001:2022
- **SOC 2 Type 2 control framework**, including relevant Trust Services Criteria (TSC)
- **Operational, technical, and administrative controls** implemented to manage information security, privacy, risk, and compliance

2.1 Functional Scope

The procedure covers internal audits across all relevant functions and domains, including but not limited to:

- Information security policies and controls
- IT operations and infrastructure management
- Asset and access management
- Risk management and vulnerability handling
- Incident management and business continuity
- Vendor and third-party risk management
- Privacy and data protection practices
- Human resources and onboarding/offboarding
- Physical and environmental security controls

2.2 Organizational Scope

This procedure applies to:

- All business units, departments, and support functions within [ORG NAME]
- All locations, including headquarters, branch offices, data centres, and remote sites
- Any personnel (permanent, contractual, or third-party) responsible for implementing or supporting ISMS/SOC 2 controls

2.3 Applicability

- This procedure is applicable for **planned audits**, **ad-hoc audits**, **compliance readiness reviews**, and **follow-up audits** related to previous nonconformities or incidents.
- It does not apply to **external certification or surveillance audits**, which are governed separately.

3. TERMS AND DEFINITIONS

Term	Definition
Internal Audit	A systematic, independent, and documented process for evaluating whether ISMS or SOC 2 controls are effectively implemented and maintained.
Audit Programme	A set of one or more audits planned for a specific timeframe, based on risk, regulatory scope, and business priorities.
Audit Plan	A detailed plan that defines the objectives, scope, criteria, methods, and schedule for a specific internal audit.
Auditor	A qualified and impartial person appointed to perform internal audits; may be internal staff or an independent consultant.
Auditee	The person, team, or function being audited. Responsible for providing information and cooperating during the audit process.
Nonconformity	A deviation from defined policies, procedures, control requirements, or compliance obligations.
Major Nonconformity	A serious failure of the ISMS/SOC 2 control that could result in significant risk exposure or a breakdown of control effectiveness.
Minor Nonconformity	A partial deviation or isolated issue that does not pose a significant risk but requires corrective action.
Observation	A noted area of weakness, inefficiency, or improvement opportunity that is not a formal nonconformity.
Corrective Action	A documented activity taken to eliminate the root cause of a nonconformity and prevent recurrence.
Follow-up Audit	A focused audit was conducted to verify whether previously identified nonconformities have been resolved effectively.

Audit Evidence	Records, statements, or data (interviews, screenshots, logs, documents) used to verify that audit criteria have been met.

4. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Chief Information Security Officer (CISO)	- Owns the Internal Audit Procedure.- Reviews and approves the annual audit programme.- Reviews high-risk findings and ensures appropriate escalation.- Reports audit outcomes to senior management or the ISMS Steering Committee.
Internal Audit Manager / Audit Lead	- Plans and coordinates internal audits based on the approved programme.- Ensures impartiality and competence of auditors.- Assigns auditors, defines audit scope, and ensures adherence to the procedure.- Reviews audit reports, findings, and follow-up activities.
Internal Auditor(s)	- Conduct assigned audits objectively and independently.- Collect, evaluate, and document audit evidence.- Identify and classify nonconformities or observations.- Prepare audit reports and present findings.
Auditee (Process Owner / Team Lead)	- Cooperate during the audit by providing access to people, processes, and evidence.- Address nonconformities through root cause analysis and corrective actions.- Provide implementation evidence for follow-up audits.
Risk & Compliance Team	- Support audit scope alignment with regulatory and contractual requirements.- Maintain the audit calendar, nonconformity register, and corrective action tracker.- Validate and monitor closure of corrective actions.
ISMS Manager	- Coordinate ISMS-specific audit activities.- Ensure ISMS scope coverage, risk-based prioritization, and alignment with ISO 27001 objectives.- Assist with communication and awareness of audit expectations.

Executive Management / ISMS Steering Committee	- Review critical audit results and unresolved risks.- Approve significant corrective action plans and resourcing.- Drive accountability and continual improvement.

5. AUDIT PRINCIPLES AND INDEPENDENCE

[ORG NAME] shall ensure that all internal audits are conducted objectively, professionally, and without bias. The following principles shall govern the conduct of all internal audits:

5.1 Audit Principles

All internal audits shall be based on the following core principles:

- **Objectivity**: Auditors shall collect and evaluate evidence based on facts, notassumptions or opinions.
- **Evidence-based approach**: Findings shall be supported by verifiable, sufficient, and appropriate audit evidence.
- **Consistency**: Audits shall follow standardized methods, checklists, and reporting formats.
- **Risk orientation**: Audit focus shall be prioritized based on the criticality of processes, control maturity, and past incidents or findings.
- **Confidentiality**: All audit data and findings shall be handled confidentially and disclosed only to authorized personnel.

5.2 Independence and Impartiality

- Internal audits shall be conducted by auditors **independent** of the area being audited to avoid conflict of interest.
- Auditors must not audit their own work or areas for which they are directly responsible.
- The Internal Audit Manager shall ensure auditor assignments maintain impartiality and competence.
- External consultants or independent internal teams may be used to ensure objectivity, especially for critical or sensitive audits (e.g., data privacy, privileged access).

5.3 Auditor Competence

- Auditors must possess adequate knowledge of:
    a. ISO/IEC 27001:2022 controls
    b. SOC 2 Trust Services Criteria
    c. Information security risks, compliance, and internal control frameworks
- Auditors shall undergo periodic training or certifications in internal auditing and ISMS standards, as required by the organization.

6. AUDIT PLANNING

[ORG NAME] shall establish a structured and risk-based approach to internal audit planning to ensure all relevant processes, systems, and controls are evaluated at appropriate intervals.

6.1 Annual Audit Programme

- An **Internal Audit Programme** shall be developed **annually** and approved by the CISO or ISMS Steering Committee.
- The programme shall define:
    - Functions or departments to be audited
    - Frequency of audits
    - Audit types (e.g., ISMS audits, SOC 2 control testing, process audits, technical audits)
    - Assigned auditors and timelines

6.2 Risk-Based Audit Prioritization

- Audit coverage and frequency shall be determined based on:
    - Business criticality of the function or asset
    - Regulatory and contractual obligations (e.g., ISO 27001, SOC 2, DPDP Act)

- Results from past audits or incident investigations
- Known or emerging risks in the function or environment
- Changes in technology, processes, or organizational structure

High-risk or high-impact areas may be audited more frequently than low-risk or support functions.

6.3 Unplanned or Trigger-Based Audits

Ad-hoc audits may be initiated in response to:

- Major security incidents or policy violations
- Whistleblower complaints or internal escalations
- Regulatory inquiries or client requests
- Mergers, acquisitions, or technology transitions

Such audits shall be recorded in the audit log with justification and approvals.

6.4 Audit Plan Communication

- A detailed **Audit Plan** for each audit engagement shall be documented and shared in advance with the auditee(s).
- The Audit Plan shall include:
  - Audit scope, objectives, and criteria
  - Tentative schedule and duration
  - Auditors assigned
  - Documentation or access required
  - Rules of engagement and confidentiality terms

7. AUDIT PROGRAMME

The Internal Audit Programme defines the overall structure, frequency, and scope of audits to be conducted across [ORG NAME] during a defined audit cycle (typically one calendar year). It ensures that all key areas of the ISMS and SOC 2 framework are audited systematically and consistently.

7.1 Programme Objectives

The objectives of the Internal Audit Programme are to:

- Verify conformity with ISO/IEC 27001:2022 and SOC 2 Trust Services Criteria
- Ensure controls are operating effectively across all departments, locations, and technologies
- Identify areas of nonconformity, weakness, or improvement
- Support management reviews, external audits, and certification efforts
- Promote a culture of continual improvement and accountability

7.2 Coverage Areas

The audit programme shall include, at a minimum:

- **ISMS core domains**:
    - Risk assessment and treatment
    - Asset management and access controls
    - Incident management
    - Cryptography and secure communications
    - Physical and environmental security
- **SOC 2 control areas** (as applicable):
    - Logical and physical access
    - Change management
    - System operations
    - Risk mitigation
    - Confidentiality and privacy practices
- **Cross-functional processes**:

- HR and onboarding/offboarding
- Vendor management and due diligence
- IT operations and DevSecOps
- Data protection and privacy compliance

7.3 Frequency

- The entire ISMS scope and SOC 2 control environment must be covered **within each annual cycle**, either through a single comprehensive audit or a series of audits based on risk and function.
- Additional audits may be conducted based on:
  - Material changes to the environment (e.g., mergers, tech migrations)
  - Significant incidents or control failures
  - Client, regulator, or certification body requirements

Note: While audit frequency may vary **per function or domain** based on risk, **no control or process within the ISMS scope shall remain unaudited for more than 12 months**.

7.4 Types of Audits Included

The programme may include:

Audit Type	Purpose
Process Audits	Evaluate control implementation in a specific department or process
Thematic Audits	Focus on specific control domains (e.g., access control, patch management)
Compliance Audits	Assess conformance with external standards like ISO 27001, SOC 2, or DPDP

Technical Audits	Review systems, configurations, and logs against baseline or hardening standards
Follow-up Audits	Re-assess closure of previous findings or corrective actions

7.5 Ownership and Updates

- The Internal Audit Programme shall be owned and maintained by the Audit Lead in collaboration with the ISMS Manager.
- The programme shall be reviewed annually or upon:
    - Major security incidents
    - Organizational restructuring
    - Changes in regulatory obligations
    - Recommendations from the management review

8. AUDIT PREPARATION AND NOTIFICATION

Proper planning and communication are essential for ensuring an efficient and cooperative internal audit process. [ORG NAME] shall follow a formalized preparation and notification process prior to each audit engagement.

8.1 Pre-Audit Preparation

The Audit Lead shall perform the following activities before initiating an internal audit:

- **Define the audit scope**: Based on the audit programme, risk priorities, and operational changes.
- **Confirm audit objectives and criteria**: Align with ISO/IEC 27001:2022 clauses, SOC 2 Trust Services Criteria, internal policies, and contractual requirements.
- **Prepare audit checklist or tools**: Tailored to the area/process being audited, using standardized templates and past audit data.
- **Assign audit team members**: Ensure independence, objectivity, and subject matter competence.

- **Review previous audit reports and corrective actions** (if applicable): For follow-up planning and contextual understanding.

8.2 Audit Notification

- The auditee shall receive a **formal audit notification email** at least **5–10 business days in advance** (or as defined by the audit programme).

- The notification shall include:

    - Audit scope, date(s), and time
    - Assigned auditor(s)
      Expected duration
    - Information or access requirements
    - Guidelines for interviews and evidence sharing
    - Confidentiality and conduct expectations

In case of ad-hoc or trigger-based audits (e.g., post-incident or complaint-driven), the notification period may be shortened based on urgency and management approval.

8.3 Audit Entry Meeting

- An **opening meeting** shall be conducted at the start of each audit to:

    - Introduce auditors and auditees

    - Review audit objectives, scope, and methodology

    - Confirm logistical arrangements and availability of evidence

    - Clarify any concerns or queries from the auditee side

The entry meeting shall be documented as part of the audit record.

9. AUDIT EXECUTION

[ORG NAME] shall conduct internal audits in a structured, evidence-based, and impartial manner to evaluate the effectiveness of implemented controls and compliance with applicable standards and policies.

9.1 Audit Methods

Auditors shall use a combination of the following methods to gather sufficient and appropriate audit evidence:

- **Interviews**: Discussions with personnel responsible for implementing or managing controls.
- **Documentation review**: Evaluation of policies, procedures, records, and logs against defined audit criteria.
- **Observation**: On-site or virtual observation of processes, tools, or system configurations in action.
- **Sampling**: Review of representative samples of transactions, tickets, logs, or records to validate consistent control application.
- **Technical validation**: Where applicable, direct verification of access controls, system settings, configurations, or other technical evidence.

9.2 Audit Criteria

Each audit shall evaluate conformity against:

- ISO/IEC 27001:2022 controls applicable to the auditee's function or process
- SOC 2 Trust Services Criteria (where applicable)
- [ORG NAME]'s internal security policies, procedures, and guidelines
- Regulatory or contractual obligations (e.g., DPDP Act, GDPR, client-specific requirements)

9.3 Evidence Documentation

- All observations, interviews, and collected artifacts shall be documented as audit evidence.
- Evidence must be:
    - Relevant, reliable, and sufficient
    - Attributable to the control or process being audited
    - Stored securely and retained as per audit record retention guidelines

9.4 Audit Observations and Findings

During execution, the auditor shall:

- Record **conformities**, **nonconformities**, and **opportunities for improvement (OFIs)**
- Classify nonconformities as **Major**, **Minor**, or **Observation** based on defined criteria (detailed in Section 11)
- Discuss observations in real-time with the auditee to validate accuracy and context

9.5 Audit Exit Meeting

- At the conclusion of fieldwork, an **exit meeting** shall be conducted with the auditee and relevant stakeholders to:
    - Present preliminary findings
    - Clarify open points or evidence gaps
    - Discuss next steps and timelines for the audit report and corrective actions

Minutes of the exit meeting shall be documented and included in the audit record.

10. AUDIT REPORTING

Following the completion of audit fieldwork, a formal audit report shall be prepared to document the findings, observations, and overall assessment of the audited area. The report shall provide actionable insights and serve as an official record for compliance tracking and management review.

10.1 Report Preparation

- The Internal Auditor or Audit Lead shall prepare the audit report within **5–10 business days** of the audit closure.
- The report shall follow a standardized format and include:
    - Audit title, date, and reference ID
    - Audit scope, objectives, and criteria
    - Auditors and participants
    - Summary of methodology and coverage

- List of **nonconformities** (classified as Major or Minor)
- **Observations** or opportunities for improvement (OFIs)
- Summary of evidence collected
- Recommendations and required corrective actions
- Agreed timelines and responsible owners
- Date of exit meeting and acknowledgement by the auditee

10.2 Finding Classifications

Finding Type	Description
Major Nonconformity	A significant failure in the implementation or effectiveness of a control, process, or policy that may result in serious risk exposure or non-compliance.
Minor Nonconformity	A partial or isolated failure that does not represent a breakdown of control but requires correction.
Observation / OFI	A potential improvement area or inefficiency that, if addressed, may enhance control maturity or audit readiness.

Note: Classifications shall be consistent with ISO/IEC 27001 and SOC 2 control language where applicable.

10.3 Report Distribution

- Finalized reports shall be shared with:
  - Auditee / Process Owner
  - ISMS Manager
  - CISO
  - Risk & Compliance Team
  - Any relevant department heads or leadership (based on impact)

- For critical functions or high-risk findings, the report shall also be escalated to the **ISMS Steering Committee** or **Executive Management**.

10.4 Audit Report Retention

- All reports, checklists, supporting evidence, and exit meeting records shall be retained securely for **a minimum of 5 years**, or longer if required by regulatory or client obligations.

11. NONCONFORMITY CLASSIFICATION AND HANDLING

[ORG NAME] shall ensure that all audit nonconformities are consistently classified, documented, and addressed through a formal process of corrective action and follow-up. This ensures risk mitigation and continual improvement of the ISMS and SOC 2 control environment.

11.1 Nonconformity Classification Criteria

Classification	Definition	Examples
Major Nonconformity	A complete or systemic failure to meet a control requirement, policy, or regulation, exposing [ORG NAME] to significant operational, regulatory, or security risk.	- Missing access review for critical systems - No documented risk assessment - Repeated audit finding not addressed
Minor Nonconformity	A partial, isolated, or non-systemic lapse in control execution or documentation that does not pose immediate high risk.	- Outdated procedure with minor deviation - Delayed logging of backup verification - Missing sign-off on non-critical document

Observation / Opportunity for Improvement (OFI)	A noted weakness or inefficiency that is not a control failure but may impact long-term performance or audit readiness.	- Inconsistent ticket tagging - Lack of version control on older policies - No periodic review tracker for awareness training

11.2 Nonconformity Logging

- All findings shall be logged in the **Internal Audit Findings Register**, maintained by the Risk & Compliance Team or Audit Lead.
- Each entry shall include:
    - Unique ID
    - Classification (Major/Minor/OFI)
    - Description and impacted control/process
    - Date identified
    - Auditor and audit reference
    - Assigned owner
    - Target resolution date

11.3 Root Cause Analysis

- For each **Major** or **recurrent Minor** nonconformity, a **Root Cause Analysis (RCA)** shall be performed using structured methods (e.g., 5 Whys, Fishbone Diagram).
- RCA findings shall be reviewed by the Audit Lead or ISMS Manager to ensure clarity and validity before corrective action is approved.

11.4 Risk Rating and Prioritization

- Each nonconformity may be assigned a **risk rating** (e.g., High / Medium / Low) based on:
    - Impact on security or compliance
    - Likelihood of recurrence
    - Exposure duration
    - Legal or contractual implications

This rating may influence prioritization, timeline, and escalation level.

12. CORRECTIVE ACTION AND FOLLOW-UP

[ORG NAME] shall ensure that all nonconformities identified during internal audits are addressed through timely, effective, and documented corrective actions. Follow-up procedures shall verify whether the root cause has been eliminated, and control effectiveness restored.

12.1 Corrective Action Plan (CAP) Requirements

For each **Major** or **Minor Nonconformity**, the assigned process owner shall develop a **Corrective Action Plan (CAP)** that includes:

- Description of the corrective action to be taken
- Responsible person(s)
- Target date for implementation
- Reference to the Root Cause Analysis (if applicable)
- Supporting evidence required for closure

CAPs must be submitted within **10 business days** of audit report issuance, unless otherwise defined by the Audit Lead or CISO.

12.2 CAP Review and Approval

- The Internal Auditor or Audit Lead shall review the submitted CAP for completeness, feasibility, and risk coverage.
- For high-risk or complex findings, the CISO or ISMS Manager may require additional controls or compensating measures.
- Approved CAPs shall be tracked in the **Audit Corrective Action Tracker**.

12.3 Verification and Closure

- Once the corrective action has been implemented, the auditee shall submit evidence of completion (e.g., updated policy, ticket logs, screenshots, revised procedures).
- The Audit Lead shall verify the effectiveness of the corrective action and record the closure status.
- If the corrective action is found inadequate, the item shall remain open and may be escalated.

12.4 Follow-Up Audits

- Follow-up audits may be scheduled to validate closure of:
    - Major nonconformities
    - Repeated or high-risk minor nonconformities
    - Unresolved observations that impact critical controls
- These audits shall focus only on previously identified issues and their resolutions.

12.5 Escalation for Overdue Actions

- CAPs not implemented within the committed timeline may be escalated as follows:

Overdue Duration	Escalation Level
0–15 Days	ISMS Manager / Risk & Compliance
16–30 Days	CISO / Department Head
>30 Days or Repeat Delay	Executive Sponsor / Risk Committee

13. AUDIT RECORDS AND RETENTION

To maintain audit readiness, demonstrate due diligence, and support internal and external assessments, [ORG NAME] shall ensure that all audit-related records are securely maintained and retained in accordance with internal policies and regulatory requirements.

13.1 Audit Records to Be Maintained

The following documents and artifacts shall be retained for each internal audit:

- Approved **Annual Audit Programme**
- Audit **Plans**, **Notifications**, and **Meeting Minutes** (entry and exit)
- Audit **Checklists** or working papers
- Collected **audit evidence** (screenshots, logs, policy versions, records, etc.)
- **Audit reports**, including findings and classifications
- **Corrective Action Plans (CAPs)** and root cause analyses
- **Audit Findings Register** and **CAP Tracker**

- Follow-up audit documentation (if applicable)

13.2 Record Retention Period

- All audit records shall be retained for a minimum of **five (5) years**, unless a longer period is required by:
    - Contractual obligations (e.g., with clients or cloud partners)
    - Regulatory frameworks (e.g., DPDP, SOC 2, HIPAA)
    - Ongoing litigation, audit, or investigation

Note: Records relating to high-risk incidents or major nonconformities may be retained longer at the discretion of the CISO or Legal Team.

13.3 Storage and Access Controls

- All records shall be stored in a secure, access-controlled repository (e.g., GRC platform, encrypted shared drive, or ISMS portal).
- Access to audit records shall be limited to:
    - Audit Team
    - CISO / ISMS Manager
    - Risk & Compliance
    - Internal or external auditors (upon request)
- Audit records shall not be altered post-factum, except to correct clerical errors with documented change logs.

14. AUDIT SCHEDULE REVIEW AND UPDATES

To ensure continuous alignment with business changes, emerging risks, and compliance requirements, [ORG NAME] shall periodically review and update its Internal Audit Schedule and Programme.

14.1 Annual Audit Programme Review

- The **Internal Audit Programme** shall be reviewed **annually** by the Audit Lead and approved by the CISO or ISMS Steering Committee.
- The review shall assess:
    - Completion status of the previous year's audit activities
    - Coverage across all ISMS domains and SOC 2 control areas
    - Trends in findings, recurring issues, or audit fatigue
    - Resource availability and skill requirements
    - Input from management reviews, risk assessments, or incidents

14.2 Adjustment Triggers

The Audit Programme may be updated mid-cycle in response to:

- Significant changes in infrastructure, processes, or ownership
- Introduction of new legal, regulatory, or client requirements (e.g., DPDP Act, new SOC 2 criteria)
- Security breaches or near misses
- Major findings from external or surveillance audits
- Mergers, acquisitions, or business expansion into new geographies or services

14.3 Communication of Changes

- Approved changes to the audit schedule shall be:
    - Documented in the updated audit calendar

- Communicated to all affected business units and auditors
- Integrated into the GRC system or audit tracking tools

- Any deferments or rescheduling of audits must be approved by the CISO and justified with written rationale.

15. PROCEDURE EXCEPTIONS

[ORG NAME] acknowledges that, under limited and justifiable circumstances, deviations from the defined Internal Audit Procedure may be necessary. In such cases, a formal exception process shall be followed to ensure risk visibility, accountability, and temporary controls.

15.1 Valid Exception Scenarios

Exceptions may be considered in scenarios such as:

- Temporary unavailability of key personnel or resources (e.g., extended leave, major outages)
- Mergers, acquisitions, or structural changes in progress
- Overlapping internal or external audit activities (e.g., certification audit, SOC 2 attestation)
- Unforeseen business disruptions (e.g., natural disasters, public emergencies)
- Planned infrastructure migration causing audit timing conflicts

15.2 Exception Request Process

- Exceptions must be formally requested by the **Audit Lead**, **ISMS Manager**, or relevant **Department Head**.
- The request must include:
  - Description of the requirement being deferred or waived
  - Business justification
  - Impact assessment (including risks to ISMS or SOC 2 compliance)
  - Proposed timeline or alternate schedule

- Compensating controls (if applicable)

15.3 Approval Workflow

Risk Level of Impacted Area	Approver
Low/Operational Functions	ISMS Manager
Medium-Risk Areas	CISO
High-Risk or Critical Controls	Executive Management / Risk Committee

Approved exceptions shall be logged in the **Audit Exception Register** and tracked for closure or re-alignment.

15.4 Time-Bound Validity and Monitoring

- Exceptions must be **time-bound** and shall not exceed **90 days** unless extended with documented justification and re-approval.
- All active exceptions shall be reviewed monthly by the Audit Lead or Risk & Compliance Team to ensure risk is contained.

16. COMPLIANCE AND ENFORCEMENT

All personnel involved in the internal audit process, including auditees and support staff, are required to comply with the provisions of this procedure. Non-compliance may impact the organization's certification status, audit readiness, and risk posture.

16.1 Internal Compliance Expectations

All departments and employees shall:

- Cooperate fully during internal audits by providing timely access to systems, documentation, and personnel.
- Respond to audit findings by completing root cause analysis and implementing corrective actions within committed timelines.

- Participate in audit interviews, awareness programs, or remediation planning as required.

- Avoid attempts to conceal evidence, obstruct audits, or retaliate against auditors or whistleblowers.

16.2 Auditor Responsibilities

Auditors shall:

- Follow the procedure with professionalism, impartiality, and confidentiality.

- Maintain objectivity and avoid conflicts of interest.

- Report any pressure, obstruction, or integrity issues to the CISO or Risk Committee.

16.3 Consequences of Non-Compliance

Violation Type	Examples	Potential Consequences
Audit Obstruction	Refusal to provide access, withholding information, non-cooperation	Escalation to CISO, disciplinary action
Ignoring CAP Timelines	Repeated failure to implement corrective actions	Management escalation, audit rating downgrade
Auditor Misconduct	Breach of confidentiality, bias, falsification of evidence	Removal from audit role, HR disciplinary action
Persistent Non-Compliance	Ignoring audit findings over multiple cycles	Escalation to Executive Management or Risk Committee

16.4 Whistleblower Protection

- Any individual may confidentially report audit-related violations or unethical conduct to:

    - The Information Security Office

- Risk & Compliance Team
- Whistleblower/ethics hotline

- [ORG NAME] prohibits retaliation against any person who raises a concern in good faith.

17. DOCUMENT CONTROL

This section defines the ownership, versioning, and maintenance process for the Internal Audit Procedure to ensure it remains current, accurate, and aligned with applicable standards and organizational requirements.

17.1 Ownership and Responsibility

Role	Responsibility
Policy Owner	Chief Information Security Officer (CISO)
Procedure Custodian	Internal Audit Manager / ISMS Manager
Approving Authority	ISMS Steering Committee / Executive Management

The Policy Owner is responsible for ensuring the procedure is implemented and enforced. The Custodian is responsible for periodic review, updates, and change documentation.

17.2 Review Frequency

- This procedure shall be reviewed **at least once every 12 months**.
- Reviews may also be triggered by:
  - Changes to ISO/IEC 27001, SOC 2, or other applicable standards
  - Audit findings related to the audit process itself
  - Structural or operational changes in [ORG NAME]'s environment

17.3 Version Control and Change Log

- All updates to the document must follow [ORG NAME]'s defined policy change process.
- Each version shall include:
    - Version number and date
    - Summary of changes
    - Reviewer and approver details

Superseded versions shall be archived and retained for **a minimum of 5 years**.

17.4 Distribution and Access

- The latest approved version of this procedure shall be:
    - Published in the organization's internal policy repository or GRC system
    - Communicated to all audit personnel and relevant stakeholders
    - Referenced during internal auditor onboarding and training

Access shall be restricted to authorized personnel only, with editing rights limited to the Policy Owner and Custodian.

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO