INFOSECTRAIN

Azpirant TECHNOLOGIES

ISO 27001:2022

AUDIT CHARTER

(Sample)

INFORMATION SECURITY AUDIT CHARTER

ISO 27001:2022 Implementation

1. INTRODUCTION

This charter establishes the framework for conducting information security audits at **INFOSECTRAIN**. It outlines the purpose, authority, and responsibilities of the internal audit function in relation to our ISO 27001:2022 Information Security Management System (ISMS).

2. PURPOSE

The Information Security Audit function provides independent assurance that our security controls are effective, our risks are properly managed, and our ISMS meets ISO 27001:2022 requirements. We support INFOSECTRAIN by:

- Verifying compliance with ISO 27001:2022 standards
- Identifying security control improvements
- Assessing and reducing information security risk
- Supporting certification maintenance
- Promoting security awareness throughout the organization

3. PROFESSIONAL STANDARDS

Our audit team adheres to:

- The Institute of Internal Auditors' International Standards
- ISO 19011:2018 Guidelines for Auditing Management Systems
- ISO/IEC 27007:2020 Guidelines for ISMS auditing
- INFOSECTRAIN Code of Ethics and Information Security Policies

4. AUTHORITY AND ACCESS

To fulfill their responsibilities, the audit team is authorized to:

- Access all information, systems, personnel, and facilities relevant to audits
- Review all documents and records related to the ISMS
- Interview staff and relevant third parties
- Observe security operations and activities
- Determine appropriate audit scope, timing, and techniques
- Obtain assistance from personnel in audited areas
- Escalate significant issues to senior management when necessary.
- All access privileges will be used solely for audit purposes and in accordance with confidentiality requirements.

5. OBJECTIVITY

The audit function maintains independence through:

- Reporting functionally to the Board/Audit Committee
- Administrative reporting to the CEO/CISO
- Having no operational responsibility for areas being audited
- Ensuring auditors do not review their own work
- Implementing auditor rotation when feasible
- Requiring disclosure of potential conflicts of interest
- Evidence-based decision making

Any circumstances that might impair independence or objectivity will be promptly disclosed to appropriate stakeholders.

6. SCOPE OF AUDIT ACTIVITIES

The scope of information security audits includes:

- Assessment of ISMS conformance to ISO 27001:2022
- Evaluation of security risk assessment and treatment processes
- Verification of Statement of Applicability implementation
- Review of security policies, procedures, and documentation
- Testing of control effectiveness through appropriate methods
- Evaluation of incident management processes
- Assessment of business continuity capabilities
- Verification of legal and regulatory compliance
- Follow-up on prior audit findings
- Preparation for certification and surveillance audits
- Special assessments requested by management

7. RESPONSIBILITIES

Audit Team Responsibilities:

- Develop risk-based annual audit plans
- Conduct audits according to professional standards
- Document findings with sufficient evidence
- Provide practical, value-added recommendations
- Communicate results effectively to stakeholders
- Maintain confidentiality of sensitive information
- Verify implementation of agreed remediation actions
- Maintain professional competence through continuous learning
- Coordinate with external auditors as appropriate
- Monitor emerging security risks and trends

Management Responsibilities:

- Review and approve the annual audit plan
- Allocate necessary resources for audit activities
- Provide timely access to requested information and personnel
- Respond promptly to audit findings
- Implement agreed remediation actions within established timeframes
- Inform the audit team of significant ISMS changes

8. AUDIT METHODOLOGY

Our audit process follows these key phases:

Planning Phase

- Define objectives, scope, and criteria
- Select qualified audit team members
- Review relevant documentation
- Develop appropriate audit plans and tools

Execution Phase

- Conduct opening meetings
- Gather and analyse evidence
- Document observations
- Evaluate against established criteria

Reporting Phase

- Prepare clear, concise audit reports
- Classify findings by risk level (Critical, High, Medium, Low)
- Conduct closing meetings to discuss results
- Distribute final reports to key stakeholders

Follow-up Phase

- Monitor remediation progress
- Verify effectiveness of implemented controls
- Report status to management

9. REPORTING STRUCTURE

The Information Security Audit function:

- Reports functionally to the Board/Audit Committee
- Reports administratively to the CEO/CIO/CISO
- Provides quarterly status reports to executive management
- Issues detailed reports for each completed audit
- Communicates critical findings immediately
- Delivers an annual assessment of overall ISMS effectiveness
- Presents significant findings at Information Security Committee meetings

10. PERFORMANCE EVALUATION

The effectiveness of the audit function is measured through:

- Completion rate of planned audits
- Timeliness of deliverables
- Quality of findings and recommendations
- Acceptance rate of recommendations
- Time to remediate identified issues
- Stakeholder satisfaction
- Value of risk identification
- Contribution to security improvement

11. CONTINUOUS IMPROVEMENT

The audit function commits to continuous improvement through:

- Periodic self-assessment against professional standards
- Collection of stakeholder feedback
- Refinement of methodologies based on lessons learned
- Monitoring of industry best practices
- Professional development and certification
- Participation in relevant security communities

12. CHARTER REVIEW

This charter will be reviewed annually and updated as necessary to reflect changes in regulatory requirements, organizational needs, or audit best practices. Updates require approval from the Board/Audit Committee.