ISO 27001:2022 Audit Finding Report

DOCUMENT CLASSIFICATION	Internal
VERISON	1.0
DATE	
DOCUMENT AUTHOR	**Ayaz Sabir**
DOCUMENT OWNER	

REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES

DISTRIBUTION LIST

NAME	SUMMARY OF CHANGE

APPROVAL

NAME	POSITION	SIGN

Contents

Executive Summary

Audit Overview and Objectives

[Insert comprehensive overview of the audit engagement including the primary objectives, scope boundaries, and strategic importance of the audited area within the organizational Information Security Management System. This section should provide senior management with clear understanding of why this audit was conducted and what it aimed to achieve.]

The audit of [Insert Audit Area/System/Process] was conducted as part of the annual internal audit program in accordance with ISO 27001:2022 requirements and organizational audit policies. The primary objectives included [Insert specific audit objectives such as evaluating control effectiveness, verifying compliance with policies and regulations, assessing risk management adequacy, and identifying improvement opportunities].

This audit engagement focused on [Insert specific focus areas] and was designed to provide independent assurance about [Insert specific assurance areas] while supporting organizational continuous improvement objectives and regulatory compliance requirements.

Key Findings Summary

[Insert concise summary of the most significant audit findings, organized by risk level and impact. This section should highlight critical issues requiring immediate management attention while providing balanced perspective on overall control environment effectiveness.]

Critical Findings: [Insert number] critical findings were identified that require immediate management attention and corrective action due to significant risk exposure and potential impact on organizational security posture and compliance status.

High-Risk Findings: [Insert number] high-risk findings were identified that require prompt management response and implementation of enhanced controls to address identified vulnerabilities and compliance gaps.

Medium-Risk Findings: [Insert number] medium-risk findings were identified that require management attention and corrective action within established timeframes to improve control effectiveness and reduce risk exposure.

Low-Risk Findings: [Insert number] low-risk findings were identified that represent opportunities for process improvement and enhanced operational efficiency.

Overall Assessment and Opinion

[Insert overall audit opinion based on comprehensive evaluation of control design and operating effectiveness. This section should provide clear assessment of the overall control of environment and management's effectiveness in addressing information security risks.]

Based on our comprehensive audit procedures and evaluation of audit evidence, we conclude that [Insert overall opinion such as "controls are generally effective with some areas requiring improvement" or "significant control deficiencies exist requiring immediate management attention"]. The overall control environment demonstrates [Insert assessment of control environment maturity and effectiveness].

Management has demonstrated [Insert assessment of management commitment and responsiveness] to information security management and has implemented [Insert assessment of control implementation and maintenance]. However, opportunities exist to enhance [Insert specific improvement areas] and strengthen [Insert specific control areas requiring attention].

Critical Recommendations

[Insert summary of the most important recommendations requiring immediate management attention and resource allocation. These recommendations should address the highest risk findings and provide clear guidance for priority corrective actions.

1. **[Insert Critical Recommendation Title]**: [Insert concise description of critical recommendation and expected timeline for implementation] **[Insert Critical Recommendation Title]**: [Insert concise description of critical recommendation and expected timeline for implementation]
2. **[Insert Critical Recommendation Title]**: [Insert concise description of critical recommendation and expected timeline for implementation]

1. Audit Scope and Methodology

1.1 Audit Scope Definition

[Insert detailed description of audit scope including specific systems, processes, locations, and time periods covered by the audit engagement. This section should provide clear

understanding of what was included and excluded from audit coverage.]

The audit scope encompassed [Insert specific scope elements such as business processes, information systems, physical locations, organizational units, and compliance requirements] within the period from [Insert start date] to [Insert end date]. The scope was designed to provide comprehensive coverage of [Insert key scope areas] while focusing on areas of highest risk and regulatory importance.

Included in Scope:

- [Insert specific included elements such as systems, processes, locations, personnel, and activities]
- [Insert additional scope inclusions with sufficient detail for clarity]
- [Insert compliance frameworks and regulatory requirements covered]

Excluded from Scope:

- [Insert specific exclusions with rationale for exclusion]
- [Insert additional exclusions and reasons for exclusion]
- [Insert any limitations or constraints that affected scope coverage]

The scope boundaries were established based on [Insert rationale for scope definition such as risk assessment results, regulatory requirements, management requests, and resource constraints] and were approved by [Insert approval authority] prior to audit commencement.

1.2 Audit Methodology and Standards

[Insert comprehensive description of audit methodology including professional standards followed, audit procedures performed, and evidence collection approaches used throughout the audit engagement.]

The audit was conducted in accordance with [Insert applicable professional standards such as IIA Standards, ISACA Guidelines, ISO 19011, and organizational audit policies] and followed established audit methodology including risk-based planning, systematic evidence collection, and comprehensive analysis and evaluation procedures.

Audit Procedures Performed:

- Risk assessment and control evaluation to identify areas requiring detailed testing and validation
- Document review and analysis including policies, procedures, system documentation, and compliance records
- Interviews with key personnel including management, system administrators, and end users
- Observation of processes and control activities to assess implementation and

operational effectiveness

- Testing of control design and operating effectiveness through sampling and detailed examination
- System configuration review and technical assessment of security controls and settings
- Compliance verification through examination of records, reports, and supporting documentation

Evidence Collection and Analysis:

Evidence collection activities included [Insert specific evidence collection methods and sources] and were designed to provide sufficient, reliable, and relevant evidence to support audit conclusions and recommendations. All evidence was evaluated for adequacy and reliability using professional judgment and established evaluation criteria.

1.2 Audit Timeline and Resources

[Insert information about audit timeline, resource allocation, and any significant events or constraints that affected audit execution.]

The audit was conducted over [Insert duration] from [Insert start date] to [Insert completion date] and required [Insert total audit hours] of audit effort. The audit team consisted of [Insert team composition and expertise areas] and was supported by [Insert any external resources or specialized expertise utilized].

Key Audit Milestones:

- Planning and preparation: [Insert dates and activities]
- Fieldwork execution: [Insert dates and activities]
- Analysis and evaluation: [Insert dates and activities]
- Report preparation and review: [Insert dates and activities]

2. Detailed Audit Findings

Finding 1: [Insert Finding Title]

Finding Classification: [Critical/High/Medium/Low Risk]
Control Area: [Insert applicable control area or framework reference]
ISO 27001:2022 Reference: [Insert specific clause or control reference]

2.1.1 Condition

[Insert detailed description of the current condition or situation identified during the audit. This section should provide factual, objective description of what was observed or discovered

without interpretation or judgment.]

During our audit procedures, we identified that [Insert specific condition observed]. Our testing revealed [Insert specific test results and observations] which indicates [Insert factual description of the situation without conclusions].

Specifically, we observed [Insert detailed observations including dates, systems, processes, or personnel involved] and found [Insert specific evidence or documentation reviewed]. The current state of [Insert relevant control or process] demonstrates [Insert objective description of current condition].

2.1.2 Criteria

[Insert description of the applicable criteria, standards, policies, or requirements that establish the expected condition or performance level. This section should clearly identify what should be in place or how the process should operate.]

According to [Insert applicable standard, policy, or requirement], [Insert specific requirement or expectation]. The [Insert relevant framework such as ISO 27001:2022, organizational policy, or regulatory requirement] requires that [Insert specific requirement text or paraphrase].

Additionally, [Insert any additional applicable criteria such as industry best practices, regulatory requirements, or organizational standards] establishes that [Insert additional requirements or expectations]. Management has also established [Insert any internal policies or procedures] that specify [Insert internal requirements or expectations].

2.1.3 Cause

[Insert analysis of the root cause or underlying reasons for the identified condition. This section should identify why the condition exists and what factors contributed to the gap between current condition and established criteria.]

Our analysis indicates that the identified condition resulted from [Insert root cause analysis results]. The primary contributing factors include [Insert specific factors such as inadequate procedures, insufficient training, resource constraints, or system limitations].

Further investigation revealed [Insert additional causal factors such as process design issues, communication gaps, or oversight deficiencies]. The underlying causes appear to be [Insert fundamental issues such as policy gaps, training deficiencies, or resource allocation problems] which have resulted in [Insert description of how causes led to current condition].

2.1.4 Effect

[Insert description of the actual or potential impact of the identified condition on organizational

objectives, security posture, compliance status, or operational effectiveness. This section should quantify impact where possible and explain significance.]

The identified condition creates [Insert specific risks or impacts such as security vulnerabilities, compliance violations, or operational inefficiencies]. The potential impact includes [Insert detailed impact analysis including financial, operational, regulatory, and reputational consequences].

Specifically, this condition may result in [Insert specific potential consequences such as unauthorized access, data breaches, regulatory penalties, or business disruption]. The risk exposure is estimated at [Insert risk assessment results including likelihood and impact ratings] and could affect [Insert affected stakeholders, systems, or processes].

Without corrective action, the organization faces [Insert long-term consequences and escalating risks] which could compromise [Insert affected objectives such as security posture, compliance status, or business operations].

2.1.5 Recommendation

[Insert specific, actionable recommendations for addressing the identified condition and underlying causes. Recommendations should be practical, cost-effective, and aligned with organizational capabilities and constraints.]

We recommend that management implement the following corrective actions to address the identified condition and underlying causes:

Immediate Actions (Within 30 days):

- [Insert specific immediate actions required to address urgent risks or compliance issues]
- [Insert additional immediate actions with clear implementation guidance]

Short-term Actions (Within 90 days):

- Insert specific short-term corrective actions to address root causes and implement sustainable solutions]
- [Insert additional short-term actions with implementation guidance and success criteria]

Long-term Actions (Within 180 days):

- [Insert strategic actions to enhance control environment and prevent recurrence]
- [Insert additional long-term improvements and capability enhancements]

2.1.6 Management Response

[Insert space for management response including agreement/disagreement with finding, proposed corrective actions, responsible parties, and implementation timeline. This section will be completed by management during the response process.]

Management Agreement: [To be completed by management]

Proposed Corrective Actions: [To be completed by management]

Responsible Party: [To be completed by management]

Target Completion Date: [To be completed by management]

Implementation Plan: [To be completed by management]

Finding 2 : [Insert Finding Title]

Finding Classification: [Critical/High/Medium/Low Risk]
Control Area: [Insert applicable control area or framework reference]
ISO 27001:2022 Reference: [Insert specific clause or control reference]

2.2.1 Condition

[Insert detailed description of the second finding following the same format and structure as Finding 1. Each finding should be thoroughly documented with sufficient detail to support audit conclusions and enable effective management response.]

[Continue with same detailed structure as Finding 1, providing comprehensive documentation of condition, criteria, cause, effect, recommendation, and space for management response.]

2.2.2 Criteria

[Insert applicable criteria and requirements for the second finding.]

2.2.3 Cause

[Insert root cause analysis for the second finding.]

2.2.4 Effect

[Insert impact analysis for the second finding.]

2.2.5 Recommendation

[Insert specific recommendations for the second finding.]

2.2.6 Management Response

[Insert space for management response to the second finding.]

Finding 3: [Insert Finding Title]

[Continue with additional findings following the same comprehensive format. Include as many findings as identified during the audit, ensuring each finding is thoroughly documented and supported by appropriate evidence.]

3. Positive Observations and Best Practices

3.1 Effective Controls and Processes

[Insert description of controls and processes that are operating effectively and demonstrate good practice. This section should provide balanced perspective by recognizing effective controls and management achievements.]

During our audit, we identified several areas where controls are operating effectively and management has implemented sound practices that support organizational security objectives and compliance requirements.

Effective Access Control Implementation: [Insert specific examples of effective access controls including technical implementations, process effectiveness, and management oversight that demonstrate good practice and control maturity.]

Strong Policy Framework: [Insert examples of well-designed and effectively implemented policies that provide clear guidance and support consistent implementation of security requirements across the organization.]

Comprehensive Training Program: [Insert examples of effective training and awareness programs that demonstrate management commitment to security culture and personnel competency development.]

3.2 Management Commitment and Leadership

[Insert recognition of management commitment, leadership engagement, and organizational culture elements that support effective information security management and continuous improvement.]

Management has demonstrated strong commitment to information security through [Insert specific examples of leadership engagement, resource allocation, and strategic support for security initiatives]. The organizational culture reflects [Insert observations about security awareness, employee engagement, and management tone regarding security importance].

Leadership engagement is evident through [Insert examples of executive involvement, board oversight, and management communication about security priorities and expectations]. This commitment provides a strong foundation for continued security program maturity and effectiveness.

3.3 Innovation and Improvement Initiatives

[Insert recognition of innovative approaches, improvement initiatives, and forward- thinking practices that demonstrate organizational commitment to security excellence and continuous enhancement.]

The organization has implemented several innovative approaches to security management including [Insert examples of creative solutions, technology implementations, or process improvements that demonstrate innovation and forward thinking].

Recent improvement initiatives include [Insert examples of proactive improvements, lessons learned implementation, and capability enhancements that demonstrate commitment to continuous improvement and security maturity advancement].

4. Risk Assessment and Prioritization

4.1 Risk Rating Methodology

[Insert explanation of the risk rating methodology used to classify findings and prioritize corrective actions. This section should provide clear understanding of how risk levels were determined and what they mean for management response prioritization.]

Risk ratings for audit findings were determined using a systematic methodology that considers both the likelihood of occurrence and the potential impact of the identified conditions on organizational objectives, security posture, and compliance status.

Risk Assessment Criteria:

Critical Risk: Findings that present immediate and severe risk to organizational security, compliance, or operations requiring immediate management, attention and corrective action within 30 days.

High Risk: Findings that present significant risk requiring prompt management response and corrective action within 60 days to prevent potential security incidents or compliance violations.

Medium Risk: Findings that present moderate risk requiring management attention and

corrective action within 90 days to improve control effectiveness and reduce risk exposure.

Low Risk: Findings that present minor risk or improvement opportunities requiring management consideration and corrective action within 180 days to enhance operational efficiency and control maturity.

4.2 Overall Risk Profile Assessment

[Insert comprehensive assessment of the overall risk profile based on audit findings, including analysis of risk trends, control environment maturity, and organizational risk exposure.]

Based on our comprehensive audit procedures and findings analysis, the overall risk profile for [Insert audited area] indicates [Insert overall risk assessment such as acceptable risk with improvement opportunities, elevated risk requiring management attention, or significant risk requiring immediate action].

The distribution of findings across risk categories demonstrates [Insert analysis of finding distribution and what it indicates about control environment maturity and risk management effectiveness]. The concentration of [Insert risk level] findings in [Insert specific areas] suggests [Insert implications for management attention and resource allocation].

Risk Trend Analysis: Comparison with previous audit results indicates [Insert trend analysis including improvements, deterioration, or stable conditions] which suggests [Insert implications for ongoing risk management and control effectiveness].

4.3 Priority Action Areas

[Insert identification of priority areas requiring immediate management attention based on risk assessment results and finding analysis.]

Based on our risk assessment and findings analysis, the following areas require priority management attention and resource allocation:

Immediate Priority (Critical and High-Risk Findings):

1. [Insert priority area with brief description of required actions]
2. [Insert additional priority area with action requirements]
3. [Insert additional priority area with action requirements]
4. **Secondary Priority** (Medium-Risk Findings):
    1. [Insert secondary priority area with improvement requirements]
    2. [Insert additional secondary priority area]

Ongoing Improvement (Low-Risk Findings):

1. [Insert improvement opportunity area]

2. [Insert additional improvement opportunity]

5. Compliance Assessment

5.1 ISO 27001:2022 Compliance Status

[Insert comprehensive assessment of compliance with ISO 27001:2022 requirements based on audit findings and testing results. This section should provide clear status of compliance and identify any gaps requiring attention.]

Our audit procedures included comprehensive evaluation of compliance with applicable ISO 27001:2022 requirements within the audit scope. The assessment covered [Insert specific clauses and controls evaluated] and included testing of [Insert specific compliance areas tested].

Compliance Status Summary:

Fully Compliant: [Insert number] requirements were found to be fully compliant with established criteria and operating effectively to meet standard requirements.

Substantially Compliant: [Insert number] requirements were found to be substantially compliant with minor gaps or improvement opportunities that do not significantly impact overall compliance status.

Partially Compliant: [Insert number] requirements were found to be partially compliant with gaps requiring corrective action to achieve full compliance with standard requirements.

Non-Compliant: [Insert number] requirements were found to be non-compliant requiring immediate corrective action to address significant compliance gaps and achieve standard requirements.

5.2 Regulatory Compliance Assessment

[Insert assessment of compliance with applicable regulatory requirements including data protection laws, industry regulations, and other legal obligations within audit scope.]

The audit included evaluation of compliance with applicable regulatory requirements including [Insert specific regulations evaluated such as GDPR, HIPAA, SOX, or industry-specific requirements]. Our testing focused on [Insert specific regulatory compliance areas tested].

Regulatory Compliance Status:

- [Insert specific regulation]: [Insert compliance status and any gaps identified]
- [Insert additional regulation]: [Insert compliance status and gaps]

- [Insert additional regulation]: [Insert compliance status and gaps]

5.3 Policy and Procedure Compliance

[Insert assessment of compliance with organizational policies and procedures including evaluation of policy implementation, adherence monitoring, and effectiveness of internal controls.]

Our evaluation of compliance with organizational policies and procedures included testing of [Insert specific policies and procedures evaluated] and assessment of [Insert compliance monitoring and enforcement mechanisms].

Policy Compliance Assessment:

- Policy implementation effectiveness: [Insert assessment results]
- Adherence monitoring adequacy: [Insert assessment results]
- Exception management processes: [Insert assessment results]
- Training and awareness effectiveness: [Insert assessment results]

6. Recommendations and Action Plan

6.1 Strategic Recommendations

[Insert high-level strategic recommendations that address systemic issues, enhance overall control environment, and support long-term security program maturity and organizational objectives.]

Based on our comprehensive audit analysis and findings evaluation, we recommend the following strategic actions to enhance the overall control environment and address systemic issues identified during our audit:

Governance and Oversight Enhancement: [Insert recommendations for improving governance structures, management oversight, and strategic direction for information security management including board engagement, executive leadership, and organizational accountability.]

Risk Management Program Strengthening: [Insert recommendations for enhancing risk management capabilities including risk assessment processes, risk treatment planning, and ongoing risk monitoring and reporting mechanisms.]

Control Framework Optimization: [Insert recommendations for improving control design, implementation, and monitoring including control standardization, automation opportunities, and effectiveness measurement.]

6.2 Operational Recommendations

[Insert specific operational recommendations that address process improvements, efficiency enhancements, and day-to-day operational effectiveness within the audited area.]

Process Improvement Opportunities: [Insert recommendations for streamlining processes, eliminating redundancies, and enhancing operational efficiency while maintaining appropriate control effectiveness and compliance requirements.]

Technology Enhancement: [Insert recommendations for leveraging technology to improve control effectiveness, automate manual processes, and enhance monitoring and reporting capabilities.]

Training and Development: [Insert recommendations for enhancing personnel competency, awareness programs, and professional development to support effective control implementation and organizational security culture.]

6.3 Implementation Roadmap

[Insert comprehensive implementation roadmap that prioritizes recommendations based on risk assessment, resource requirements, and organizational capabilities while providing clear timeline and milestone expectations.]

Phase 1 - Immediate Actions (0-30 days):

- [Insert critical actions requiring immediate implementation]
- [Insert resource requirements and success criteria]
- [Insert responsible parties and accountability measures]

Phase 2 - Short-term Implementation (30-90 days):

- [Insert short-term corrective actions and improvements]
- [Insert implementation planning and resource allocation]
- [Insert monitoring and progress measurement approaches]

Phase 3 - Long-term Enhancement (90-180 days):

- [Insert strategic improvements and capability enhancements]
- [Insert sustainability planning and ongoing maintenance requirements]
- [Insert performance measurement and continuous improvement integration]

6.4 Success Metrics and Monitoring

[Insert specific metrics and monitoring approaches for measuring implementation progress, effectiveness of corrective actions, and achievement of improvement objectives.]

Implementation Progress Metrics:

- Corrective action completion rates and timeline adherence
- Resource utilization and budget performance
- Stakeholder engagement and satisfaction levels
- Milestone achievement and deliverable quality

Effectiveness Measurement:

- Control performance improvement indicators
- Risk reduction and exposure mitigation results
- Compliance status enhancement and gap closure
- Operational efficiency and process improvement outcomes

7. Management Response and Action Plan

7.1 Management Response Summary

[Insert space for comprehensive management response to audit findings and recommendations including overall agreement, resource commitment, and implementation approach. This section will be completed by management during the response process.]

Overall Management Response: [To be completed by management - should include acknowledgment of findings, commitment to corrective action, and strategic approach to implementation]

Resource Commitment: [To be completed by management - should specify resource allocation, budget approval, and personnel assignment for corrective action implementation]

Implementation Approach: [To be completed by management - should outline management's approach to addressing findings, timeline expectations, and coordination mechanisms]

7.2 Detailed Action Plan

Insert detailed action plan matrix showing specific corrective actions, responsible parties, target completion dates, and success criteria for each audit finding and recommendation.]

Finding/ Recommendation	Corrective Action	Responsible Party	Target Date	Success Criteria	Status
[Finding 1]	[Specific action]	[Name/Title]	[Date]	[Criteria]	[status]
[Finding 2]	[Specific action]	[Name/Title]	[Date]	[Criteria]	[status]
[Finding 3]	[Specific action]	[Name/Title]	[Date]	[Criteria]	[status]

7.3 Implementation Timeline and Milestones

[Insert comprehensive implementation timeline showing key milestones, dependencies, and critical path activities for successful corrective action implementation.]

30-Day Milestones:

- [Insert specific 30-day milestones and deliverables]
- [Insert responsible parties and success criteria]

60-Day Milestones:

- [Insert specific 60-day milestones and deliverables]
- [Insert progress measurement and validation approaches]

90-Day Milestones:

- [Insert specific 90-day milestones and deliverables]
- [Insert effectiveness assessment and sustainability planning]

7.4 Monitoring and Follow-up Plan

[Insert plan for ongoing monitoring of corrective action implementation, progress reporting, and follow-up audit activities to verify effectiveness of implemented solutions.]

Progress Reporting: [Insert reporting frequency, format, and recipients for

implementation progress updates]

Monitoring Activities: [Insert specific monitoring activities, responsible parties, and performance indicators for tracking implementation effectiveness]

Follow-up Audit Planning: [Insert timeline and scope for follow-up audit activities to verify corrective action implementation and effectiveness]

8. Conclusion and Next Steps

8.1 Overall Audit Conclusion

[Insert comprehensive conclusion that summarizes audit results, overall assessment of control environment, and key messages for management and stakeholders.]

Based on our comprehensive audit procedures and evaluation of audit evidence, we conclude that [Insert overall conclusion about control environment effectiveness, compliance status, and organizational security posture]. The audit identified [Insert summary of findings and their significance] while recognizing [Insert positive observations and effective controls].

The overall control environment demonstrates [Insert assessment of control maturity and effectiveness] with [Insert specific strengths and areas for improvement]. Management's commitment to [Insert assessment of management engagement and responsiveness] provides a strong foundation for addressing identified issues and enhancing security program effectiveness.

8.2 Key Success Factors

[Insert identification of key factors that will contribute to successful implementation of audit recommendations and achievement of improvement objectives.]

Successful implementation of audit recommendations will depend on [Insert critical success factors such as management commitment, resource allocation, stakeholder engagement, and change management effectiveness]. Key factors include:

- **Leadership Commitment**: [Insert importance of executive support and resource commitment]
- **Cross-functional Collaboration**: [Insert need for coordination across organizational units]
- **Change Management**: [Insert importance of effective change management and communication]
- **Continuous Monitoring**: [Insert need for ongoing monitoring and adjustment]

8.3 Future Audit Considerations

[Insert recommendations for future audit planning, scope adjustments, and areas requiring ongoing attention based on audit results and organizational changes.] Future audit activities should consider [Insert recommendations for future audit focus areas, scope adjustments, and timing considerations based on audit results and organizational risk profile changes].

Recommended Future Audit Focus:

- [Insert specific areas requiring ongoing audit attention]
- [Insert emerging risks or changes requiring future audit coverage]
- [Insert follow-up audit requirements and timing]

8.4 Acknowledgments

[Insert acknowledgment of cooperation and support received during the audit engagement from management, staff, and other stakeholders.]

We acknowledge the cooperation and support provided by [Insert specific acknowledgments for management, staff, and other stakeholders who contributed to audit success]. The professional and collaborative approach demonstrated throughout the audit engagement facilitated effective audit execution and comprehensive evaluation of control effectiveness.

Appendices

Appendix A: Audit Testing Summary

[Insert summary of audit testing performed including sample sizes, testing methodologies, and detailed test results that support audit findings and conclusions.]

Control Area	Tests Performed	Sample Size	Results Summary	Exceptions Noted
[Control Area 1]	[Test description]	[Size]	[Results]	[Exceptions]
[Control Area 2]	[Test description]	[Size]	[Results]	[Exceptions]
[Control Area 3]	[Test description]	[Size]	[Results]	[Exceptions]

Appendix B: Documentation Reviewed

[Insert comprehensive list of documents, records, and other materials reviewed during the audit engagement.]

Policies and Procedures:

- [Insert list of policies and procedures reviewed]

System Documentation:

- [Insert list of system documentation and technical materials reviewed]

Compliance Records:

- [Insert list of compliance documentation and regulatory materials reviewed]

Other Materials:

- [Insert list of additional materials and evidence reviewed]

Appendix C: Personnel Interviewed

[Insert list of personnel interviewed during the audit including names, titles, and interview focus areas while maintaining appropriate confidentiality considerations.]

Name	Title	Department	Interview Focus
[Name]	[Title]	[Department]	[Focus areas]
[Name]	[Title]	[Department]	[Focus areas]
[Name]	[Title]	[Department]	[Focus areas]

Appendix D: Risk Assessment Matrix

[Insert detailed risk assessment matrix showing risk ratings, impact analysis, and likelihood assessments for all identified findings.]

Finding	Likelihood	Impact	Risk Rating	Justification
[Finding 1]	[Rating]	[Rating]	[Overall]	[Justification]
[Finding 2]	[Rating]	[Rating]	[Overall]	[Justification]
[Finding 3]	[Rating]	[Rating]	[Overall]	[Justification]

Report Distribution

- Chief Executive Officer
- Chief Information Security Officer
- [Insert specific management recipients]
- Internal Audit Committee
- Board of Directors (Executive Summary)
- External Auditors (as applicable)

Report Retention

This audit report will be retained in accordance with organizational record retention policies and regulatory requirements for a minimum of [Insert retention period] years.

Follow-up Schedule

- 30-day progress review: [Insert date]
- 60-day progress assessment: [Insert date]
- 90-day implementation verification: [Insert date]
- Follow-up audit planning: [Insert date]

This audit report contains confidential and proprietary information. Distribution is restricted to authorized recipients only. Any unauthorized disclosure or distribution is prohibited.