INSERT COMPANY NAME & DATE HERE

ISO/IEC 27001 Information Security Management Audit Report

This document, created by GSDC and provided along with GSDC Certification, offers a comprehensive audit report for ISO/IEC 27001, the international standard for Information Security Management Systems (ISMS). The audit report covers critical audit points across various categories such as organizational context, leadership, risk management, resource allocation, compliance, and continual improvement.

The report is designed to help organizations ensure that their information security management processes are aligned with industry best practices, regulatory requirements, and business objectives.

Each audit point is presented with a detailed assessment to assist auditors in evaluating the effectiveness, compliance, and maturity of the organization's information security practices. This comprehensive report provides actionable insights and recommendations to enhance the organization’s ISMS in accordance with ISO/IEC 27001 standards.

INSERT COMPANY NAME & DATE HERE

Completion Date:

Completed By:

QM Version:

Executive Summary:

Corrective Actions (CA):

Preventive Actions (PA):

Improvement Actions (IA):

KEY: **OK** = Meets criteria **C** = Comment **X** = Nonconformity

INSERT COMPANY NAME & DATE HERE

High = 1 **Intermediate** = 2 **Low** = 3

Note: **ORANGE** highlighted fields represent criteria used during the **Company Computer Systems Technical Assessment**

INSERT COMPANY NAME & DATE HERE

Action Plan:

Action Type		**Criteria**		**Priority**	
Finding					
Root Cause					
Proposed Action					
Due Date		**Task Assigned To**			
Completion Date		**Task Verified By**			
Final Action					
Action Effectiveness					

INSERT COMPANY NAME & DATE HERE

Evaluation Date		**Task Verified By**	

Action Type		**Criteria**		**Priority**	
Finding					
Root Cause					
Proposed Action					
Due Date		**Task Assigned To**			
Completion Date		**Task Verified By**			
Final Action					

INSERT COMPANY NAME & DATE HERE

Action Effectiveness			
Evaluation Date		**Task Verified By**	

INSERT COMPANY NAME & DATE HERE

Action Type		**Criteria**		**Priority**	
Finding					
Root Cause					
Proposed Action					
Due Date		**Task Assigned To**			
Completion Date		**Task Verified By**			
Final Action					
Action Effectiveness					

INSERT COMPANY NAME & DATE HERE

Evaluation Date		**Task Verified By**	

INSERT COMPANY NAME & DATE HERE

Action Type		**Criteria**		**Priority**	
Finding					
Root Cause					
Proposed Action					
Due Date		**Task Assigned To**			
Completion Date		**Task Verified By**			
Final Action					
Action Effectiveness					

INSERT COMPANY NAME & DATE HERE

Evaluation Date		**Task Verified By**	

INSERT COMPANY NAME & DATE HERE

Action Type		**Criteria**		**Priority**	
Finding					
Root Cause					
Proposed Action					
Due Date		**Task Assigned To**			
Completion Date		**Task Verified By**			
Final Action					
Action Effectiveness					

INSERT COMPANY NAME & DATE HERE

Evaluation Date		**Task Verified By**	

Action Type		**Criteria**		**Priority**	
Finding					
Root Cause					
Proposed Action					
Due Date		**Task Assigned To**			
Completion Date		**Task Verified By**			
Final Action					

INSERT COMPANY NAME & DATE HERE

Action Effectiveness	

INSERT COMPANY NAME & DATE HERE

Audit Checklist

No.	Audit Point	Detailed Requirement Description	Compliance					Reference	Objective Evidence
			OK/C/X		Action	Priority			
1	Context of the Organization	Ensure the organization has identified internal and external issues that can affect its ISMS objectives and security requirements. Review how the organization understands its context within the industry.							
2	Understanding of Stakeholders	Identify relevant stakeholders (internal and external) and their expectations with respect to information security. Ensure that these expectations have been captured and considered in the ISMS.							

INSERT COMPANY NAME & DATE HERE

3	Scope of ISMS	Verify that the scope of the ISMS is clearly defined, including boundaries and applicability, covering the systems, locations, processes, and assets that are part of the ISMS.					
4	Information Security Policy	Ensure the organization has a documented information security policy that is aligned with its business objectives and supports the ISMS. The policy should be communicated and available to all employees.					
5	Leadership and Commitment	Confirm that top management demonstrates leadership and commitment to the ISMS, ensuring resources, support, and strategic direction are provided. Review evidence of leadership involvement in ISMS meetings and decisions.					

INSERT COMPANY NAME & DATE HERE

6	Roles and Responsibilities	Check that information security roles and responsibilities are clearly defined, assigned, and communicated. Ensure that the staff understands their security-related duties.					
7	Risk Assessment Process	Review the organization's process for identifying and assessing risks to information security. Ensure that risks are evaluated using a consistent methodology and that the risk assessment is periodically reviewed.					
8	Risk Treatment Plan	Verify that the organization has a documented risk treatment plan that outlines how identified risks will be addressed, mitigated, or accepted. The plan should include control implementation responsibilities and timelines.					

INSERT COMPANY NAME & DATE HERE

9	Asset Inventory and Classification	Ensure that all information assets (data, hardware, software, etc.) are inventoried and classified based on their value, sensitivity, and criticality to the organization.					
10	Access Control Policy	Verify that access controls are in place to restrict access to sensitive information and systems. Ensure that access is granted based on the principle of least privilege, and review how access rights are managed and monitored.					
11	Security Awareness Training	Confirm that security awareness training is provided regularly to all employees. Training should cover key topics such as phishing, password management, and reporting security incidents.					
12	Human Resources Security	Review the organization's procedures for ensuring information security during hiring, training, termination,					

INSERT COMPANY NAME & DATE HERE

		or role changes of employees. Ensure that background checks, contracts, and exit procedures are documented.					
13	Physical and Environmental Security	Verify that physical security measures, such as restricted access to server rooms, security cameras, and environmental controls (e.g., fire suppression, climate control), are in place to protect information systems.					
14	Cryptography Policy	Ensure that cryptographic controls (e.g., encryption, digital signatures) are implemented to protect the confidentiality, integrity, and authenticity of sensitive information. Review the policy and usage guidelines for cryptographic techniques.					

INSERT COMPANY NAME & DATE HERE

15	Operations Security	Confirm that operational security procedures are in place to manage the day-to-day security of information systems, including system backups, malware protection, patch management, and network security.					
16	Communication Security	Review the controls in place to protect the security of information in transit, such as encryption for email, VPNs for remote access, and secure communication protocols.					
17	Supplier and Third-Party Risk Management	Verify that third-party suppliers and service providers are assessed for information security risks. Ensure that contracts include information security requirements and that third-party performance is monitored.					

INSERT COMPANY NAME & DATE HERE

18	Incident Management Process	Review the organization's incident management procedures, including how information security incidents are identified, reported, and responded to. Verify that there is an incident response plan, and that incidents are recorded and analyzed.					
19	Business Continuity and Disaster Recovery	Ensure that the organization has a business continuity and disaster recovery plan in place. The plan should outline how critical operations will continue in the event of an information security incident or major disruption.					
20	Compliance with Legal Requirements	Verify that the organization complies with relevant laws, regulations, and contractual obligations related to information security (e.g., data protection regulations, industry-specific security standards).					

INSERT COMPANY NAME & DATE HERE

21	Internal Audit Program	Ensure that regular internal audits of the ISMS are conducted to assess compliance with ISO 27001 and the organization's policies. Review audit schedules, findings, and corrective actions.					
22	Nonconformities and Corrective Actions	Check the organization's procedure for identifying nonconformities within the ISMS and taking corrective actions. Ensure that nonconformities are recorded, analyzed, and addressed in a timely manner.					
23	Management Review	Review evidence that top management regularly reviews the ISMS to ensure its continuing suitability, adequacy, and effectiveness. The review should consider the results of audits, performance metrics, incidents, and opportunities for improvement.					

INSERT COMPANY NAME & DATE HERE

24	Continual Improvement Process	Verify that there is a formal process for identifying and implementing continual improvements to the ISMS. Ensure that feedback from audits, incidents, and stakeholder inputs is used to drive improvement initiatives.					
25	Asset Ownership and Responsibility	Ensure that each information asset has an assigned owner responsible for its security throughout its lifecycle. Owners should be accountable for classifying the asset, determining access, and ensuring appropriate controls are applied.					
26	Mobile Device and Teleworking Security	Review the security controls in place for mobile devices and teleworking. Ensure that employees working remotely or using personal devices have secure access to corporate systems and data.					

INSERT COMPANY NAME & DATE HERE

27	Secure Development Practices	Verify that secure development practices are in place to ensure that software applications are developed with security in mind, including secure coding standards, code reviews, and security testing.					
28	Network Security Controls	Confirm that network security controls, such as firewalls, intrusion detection/prevention systems (IDPS), and network segmentation, are implemented to protect the organization's IT infrastructure.					
29	Vulnerability Management	Review the organization's vulnerability management process, including the identification, prioritization, and remediation of vulnerabilities in software, hardware, and systems. Ensure regular vulnerability scanning is conducted.					

INSERT COMPANY NAME & DATE HERE

30	Patch Management Process	Verify that a patch management process is in place to ensure that critical patches and updates are applied to systems and software in a timely manner to reduce security risks.					
31	Data Loss Prevention (DLP)	Check that data loss prevention measures are in place to protect sensitive information from being leaked, whether through accidental or malicious actions. This includes monitoring for unauthorized transfers of sensitive data.					
32	Information Classification Policy	Ensure that there is a formal information classification policy that defines how information is classified based on its sensitivity and value. The policy should outline handling requirements for each classification level.					

INSERT COMPANY NAME & DATE HERE

33	Data Retention and Disposal	Verify that the organization has data retention and disposal policies in place to ensure that sensitive information is retained only as long as necessary and securely disposed of when no longer needed.					
34	Logging and Monitoring	Review the organization's logging and monitoring activities to ensure that security events, access to critical systems, and user activities are recorded and reviewed for anomalies or suspicious behavior.					
35	Security Incident Reporting	Ensure that there is a defined process for reporting security incidents, including clear guidelines for who should be notified, how incidents should be documented, and the timeline for reporting.					

INSERT COMPANY NAME & DATE HERE

36	Information Security Metrics	Verify that the organization has established information security metrics to measure the effectiveness of the ISMS and security controls. Ensure that these metrics are regularly reviewed and reported to management.						
37	Authentication and Identity Management	Check that strong authentication mechanisms are in place to verify the identity of users accessing sensitive systems and information. This includes multifactor authentication (MFA) for critical systems.						
38	Password Management Policy	Ensure that a password management policy is in place and enforced. The policy should specify password complexity requirements, expiration periods, and guidance on secure password storage.						

INSERT COMPANY NAME & DATE HERE

39	Change Management Process	Verify that changes to information systems, software, or hardware are managed through a formal change management process to ensure that changes do not introduce security risks.							
40	Third-Party Contract Review	Ensure that contracts with third parties, including suppliers and service providers, include information security clauses that specify the security requirements and responsibilities of both parties.							
41	Endpoint Security Controls	Review the endpoint security measures in place to protect desktops, laptops, and other endpoints from malware, unauthorized access, and other security threats.							
42	Remote Access Security	Verify that secure methods of remote access are implemented, such as VPNs, to ensure that users accessing the organization's systems from outside the							

INSERT COMPANY NAME & DATE HERE

		network are protected.							
43	Backup and Recovery Processes	Ensure that regular backups of critical data are performed and that backup data is securely stored. Verify that recovery procedures are tested to ensure the organization's ability to restore operations after an incident.							
44	Encryption Key Management	Review the organization's procedures for managing encryption keys, including key generation, storage, distribution, and disposal. Ensure that keys are securely protected and that access to them is restricted.							
45	Malware Protection	Verify that malware protection mechanisms, such as antivirus software and endpoint protection solutions, are in place and kept up-to-date to							

INSERT COMPANY NAME & DATE HERE

		protect systems from malware threats.							
46	Privacy and Data Protection	Ensure that the organization complies with data protection and privacy regulations (e.g., GDPR). Review policies and practices related to the protection of personal and sensitive data.							
47	Cloud Security Controls	Verify that appropriate security controls are in place for data and applications hosted in the cloud. Ensure that cloud service providers are assessed for security risks and that security responsibilities are clearly defined.							
48	Internal Audit Frequency and Scope	Confirm that internal audits of the ISMS are conducted regularly and that the scope covers all critical areas, including risk management, access controls, and							

INSERT COMPANY NAME & DATE HERE

		compliance.							
49	Corrective Action Effectiveness	Review whether corrective actions taken in response to identified nonconformities are effective and have been implemented in a timely manner.							
50	Continuous Monitoring and Improvement	Ensure that the organization continuously monitors its information security environment for new risks, emerging threats, and opportunities for improvement, and adjusts the ISMS accordingly.							