Information System Audit (ISA) Manual

The Institute of Chartered Accountants of Nepal (ICAN)

Information System Audit (ISA) Manual

The Institute of Chartered Accountants of Nepal (ICAN)

Price : Rs.150.00

First Edition : June 2025

Published By : The Institute of Chartered Accountants of Nepal (ICAN)
ICAN Marg, Satdobato, Lalitpur
E-mail: ican@ntc.net.np
Website: https://en.ican.org.np/en/

Printed at : Print and Art Service
Bagbazar, Kathmandu, Tel: 5344419

Foreword

In today's era of rapid technological advancement, businesses increasingly depend on information systems to streamline operations and achieve strategic objectives. These systems—comprising people, processes, and technology—introduce unique risks that demand rigorous oversight and assessment. Recognizing this need, the Information System Audit Manual published by the Institute of Chartered Accountants of Nepal (ICAN) provides comprehensive methodologies and procedures to guide auditors in providing effective Information Systems (IS) Audit.

ICAN remains committed to enhancing the professional competence of its members by consistently organizing mandatory Continuing Professional Education (CPE) trainings, seminars, workshops, and by issuing relevant standards and guidelines. These initiatives aim to support members in delivering high-quality professional services that meet stakeholder expectations in the most efficient and effective manner. In line with this commitment, the ISA Manual has been developed based on internationally accepted frameworks, standards, guidelines, and best practices.

The Information System Audit (ISA) Manual is designed to assist members in systematically planning, conducting, and reporting information system audits. While it follows globally recognized standards and frameworks, it is acknowledged that no single manual can address every possible scenario. Accordingly, auditors are encouraged to exercise professional judgment and tailor their approaches to suit the specific risks, complexities, and contextual factors of the organization being audited—taking into account its industry, regulatory requirements, and unique operating environment.

I extend my heartfelt appreciation to Biz Serve IT for their substantial contribution for helping to give a final shape. I also commend the dedicated efforts of the ICAN management team and the various committees, especially the IT Committee and the Professional Development Committee, for their leadership in initiating, providing feedback and reviewing this important document.

My sincere gratitude also goes to all our members—particularly those certified in IS audit—who provided valuable feedback and insights during the finalization process. Finally, I wish to thank the ICAN Council members for their constructive suggestions and support in approving this manual.

I am confident that this manual will serve as a valuable resource for our members and significantly aid them in conducting high-quality information system audits.

CA. Prabin Kumar Jha

President, ICAN

Table of Contents

CHAPTER 1
OVERVIEW

1.1 About the Institute

The Institute of Chartered Accountants of Nepal (ICAN) was founded under the Nepal Chartered Accountants Act, 1997, with the aim of enhancing the accounting profession's social recognition and trust, highlighting its essential role in economic development and social responsibility. ICAN members serve in various roles, including auditing, accounting, governance, board positions, and public services. As digital landscapes evolve, the importance of strong and secure Information Systems (IS) continues to grow, ICAN, as a regulatory body, aims to bring uniformity in the standard and quality of IS audit practices.

To achieve the goal, ICAN has been supporting its members in performing IS audits. It also offers courses in Information System Audit (ISA). ICAN is highly committed to standards of professional conduct and expertise in IS auditing. As ICAN continues to adapt to the changing professional and business landscape, the knowledge and expertise of its members are crucial to maintaining a high standard in performing IS audits.

1.2 Purpose of the Manual

This manual, developed by ICAN, is a guiding document for its members. It provides a structured approach for planning, executing, and reporting on IS audits. It aligns the audit practices with internationally recognized standards and frameworks. More importantly, it highlights the domains, high-level risks, and controls on which to focus during an IS audit.

1.3 Scope of the Manual

This manual is designed as a guide for IS auditors conducting IS audits within Nepal. It establishes procedures and guidelines for conducting IS audits, taking into consideration the dynamic nature of information systems and the varied environments in which they operate. It is important to note that this manual may not encompass all potential scenarios, and adjustments may be necessary to ensure thorough and effective audits. Recognizing the need for adaptability, IS auditors are encouraged to tailor their approaches to address the specific needs, risks, and complexities based on need, context, industry, regulation, and the nature of organization.

In instances where the provided methodologies, procedures, and checklists are deemed inadequate for a particular audit engagement, ICAN encourages the IS auditors to explore alternative frameworks and methodologies. This flexibility enables the auditors to conduct comprehensive assessments to meet the unique requirements of a given industry. IS auditors can improve the standard and quality of audit engagements by following the relevant guidelines.

1.4 Information System Auditing Standard

The IT Audit Framework (ITAF) by the Information Systems Audit and Control Association (ISACA) provides a structured approach to conducting IS audits. When needed, the IS auditors are recommended to follow the standard. The framework categorizes standards into general, performance, and reporting

standards, offering a comprehensive set of guidelines for auditors to follow. Additionally, auditors may refer to Nepal Standards on Auditing (NSAs) issued by the Auditing Standards Board and ISO 19011:2018 Guidelines **for auditing management systems** for further guidance and reference.

1.5 Objectives

The objectives of this Information System (IS) Audit Manual are as follows:

- A guiding document for IS auditors: The manual serves as a guiding document for IS auditors, directing them in conducting detailed audits and delivering findings of utmost precision and reliability, to ensure the highest quality output from IS audits and reporting processes.
- To maintain uniformity and quality: The manual aims to promote consistency and quality in IS audit procedures performed by IS auditors. By following the standard practices and methodologies outlined in the manual, IS auditors can conduct audits with rigor and precision, no matter who the auditor or organization is.
- Compliance with legal provisions: One of the primary objectives of this manual is to ensure that IS auditors comply with applicable legal provisions and regulatory requirements while conducting IS audits. By verifying compliance with relevant laws and regulations, IS auditors can uphold the integrity and credibility of the audit process and its outcomes.
- Enhance stakeholders' trust: By adhering to standardized audit procedures and producing high-quality audit reports, IS auditors can enhance stakeholders' trust in the reliability and usefulness of the audit process and its outcomes. Stakeholders, including organizational leadership, regulatory bodies, and other relevant parties, can have confidence that IS audits conducted in accordance with this manual are thorough, objective, and reliable.
- Clarify scope and limitations: The manual aims to provide clarity regarding the scope and limitations of IS audits conducted by IS auditors. By clearly defining the scope of their engagements and articulating any inherent limitations or constraints, IS auditors can manage stakeholders' expectations effectively and ensure transparency throughout the audit process.
- Reference to IS domains, risks, controls, and checklists: The manual aims to provide a reference to relevant IS audit domains, and associated risks. Similarly, for each domain, it provides details on controls and checklists to be audited. However, the list, while comprehensive, may not suffice for every audit context. Therefore, it is the responsibility of the IS auditor to develop a sound understanding of IS and associated risks in order to craft the required questions.

1.6 Audience

This manual serves as a vital resource for ICAN members including IS auditors listed by ICAN and with diverse range of stakeholders involved in IS audits. This includes organizational leadership, audit committees or departments, external auditors, regulatory bodies, and other parties with an interest in ensuring the effectiveness and integrity of IS audit processes. By providing clear guidance and best practices, manual aims to support the professional development and effectiveness of IS auditors while fostering trust and confidence among stakeholders in the audit process and its outcomes.

1.7 Legal and Regulatory Framework for IS Audit

Organizations under the supervision of Nepal Rastra Bank, Nepal Telecommunication Authority, and Nepal Insurance Authority are required to conduct IS audits. Following is the industry regulations and guidelines issued by the regulators in Nepal:

1	**Banking and Fintech Industry** **Regulator:** Nepal Rastra Bank
1.1	Nepal Rastra Bank Information Technology Guidelines, 2012
1.2	Unified Directive Related to Payment System, 2080
1.3	Cyber Resilience Guidelines
2	**Insurance Industry** **Regulator:** Nepal Insurance Authority (Formerly: Beema Samiti)
2.1	Insurer IT Guidelines, 2076
2.2	Digital Insurance Policy Guidelines, 2024
3	**Telecommunication Industry** **Regulator:** Nepal Telecommunication Authority
3.1	Cyber Security Bylaw, 2077
3.2	WiFi Hotspot Operation Bylaw
3.3	Internet and Email Service Operation Bylaw

Note: Applicable regulatory acts, laws, and guidelines are subject to change. Therefore, it is the responsibility of the IS auditors to stay updated on relevant revisions.

In addition to regulatory requirements, an increasing number of organizations are proactively performing IS audits to identify the gaps and manage the associated risks. This practice has become indispensable for assessing an organization's overall information security posture and aligning its procedures with industry benchmarks. Within the ICAN audit framework, it is crucial to consider existing industry regulations and guidelines issued by regulators relevant to IS audits.

CHAPTER 2
INTRODUCTION

2.1 Objective of IS Audit

The primary objective of an IS audit is to test the effectiveness of applicable information system controls and evaluate the effectiveness of the organization's risk management process. This requires a thorough assessment of how well risks are managed through the design and implementation of appropriate controls.

2.2 Information System

An information system is a combined structure consisting of people, processes, and technology to achieve common business goals. The key functions of an information system are to collect, store, process, and share data to help in analysis, reporting, notification, coordination, and decision-making for the business. It consists of software, hardware, and network components that collect, process, store, and dispatch information.

A functional information system environment consists of three components: people, processes, and technology. The end-user must be able to use the technology as per the defined process to make data-driven decisions. Technology modifications and improvements are sometimes the most complicated parts of a business transformation. Therefore, these components should work in harmony in order to have a secure and efficient information system.

2.3 Confidentiality, Integrity and Availability

Confidentiality, integrity, and availability (the CIA triad) are the three pillars required to develop and maintain a functionally efficient and secure information system. A gap in any one of the pillars of the CIA triad means that there is an information system security control gap that poses a risk to the given infrastructure.

Information should only be accessed by authorized users or systems, while unauthorized access should always be restricted. An attacker might exploit the access control vulnerabilities to obtain sensitive information. The main defense against this is to utilize proper access control, authentication, authorization, and encryption standards.

Integrity focuses on maintaining the accuracy, reliability, and consistency of data throughout its lifecycle. Integrity is ensured when the data and information can’t be tampered with. For example, any software that we download must be trustworthy. If the integrity of the software is changed, the software is unreliable. Integrity can be compromised on purpose. An attacker can get past an intrusion detection system (IDS), modify file settings to permit illegal access, or manipulate the system's logs to perform the attack. Someone might enter the incorrect code. The use of hashing, encryption, digital certificates, or digital signatures can help to maintain the integrity of your data.

Availability is about ensuring that information and resources are accessible for use when needed. Even with the highest level of confidentiality and integrity, data and information can’t be used if

they are not accessible. Systems, networks, and applications should be up and running as they are designed.

By evaluating controls for protection of confidentiality, integrity, and availability, IS auditors can gain insight into the security posture of an organization's information systems. Therefore, it is important for an IS auditor to understand the concepts of confidentiality, integrity, and availability in order to identify gaps and vulnerabilities and provide appropriate recommendations.

2.4 Risk

There are two primary categories for information system risks:

- **Governance and Compliance Risks**

  Governance and compliance risks arise due to strategic misalignment, lack of accountability, audit misconduct, and poor third-party management. In addition, failure to comply with applicable laws, regulations, and policies in relation to business strategies also increases governance and compliance risks. Non-compliance with these can result in fines, penalties, mistrust, and legal action. IS auditors are advised to refer to the prevailing regulatory requirements applicable to Nepal mentioned in [1.7].

- **Information Security Risks**

  An information security risk is an outcome of vulnerability, threat, and impact.

  Risk = Vulnerability x Threat x Impact

  Vulnerabilities are weaknesses in the implementation of security controls. Vulnerabilities can arise from inadequate security measures, outdated software, misconfigurations, or human error. The presence of vulnerabilities increases the likelihood of a successful attack.

  A threat is a potential harm to an information system. A threat can be a malicious actor, malware, natural disasters, human error, etc. A vulnerability is exploited by a potential threat to compromise confidentiality, integrity, and availability.

  Impact refers to the consequences of an attack. The consequences can impact operations, financial losses, regulatory penalties, disruption of services, reputational damage, loss of customer trust, etc.

  From an audit perspective, understanding the security control objective involves assessing whether the implemented controls can effectively mitigate the identified risks or not. Auditors should evaluate the adequacy, effectiveness, and efficiency of security controls in addressing vulnerabilities, mitigating threats, and reducing the potential impact of security incidents. In this process, the auditors should review the design and implementation of controls, their alignment with recognized security frameworks and best practices, and their ability to address specific risks identified through risk assessments or threat modeling exercises. By evaluating security controls against the risk equation, the auditors can report any discrepancies to stakeholders, in case the organization's security posture is not appropriately aligned with its risk tolerance and is not helping to safeguard its assets and operations against potential threats and vulnerabilities.

2.5 Risk Grading

Risk Grade	Characteristics
Critical	The severity level is classified as **Critical** when controls are not in line with established control objectives, and gaps can lead to a complete system compromise if exploited. They should be fixed immediately without any delay. Successful exploitation at this level typically results in a total loss of confidentiality, integrity, and availability of data within the system. Compensatory controls are ineffective in reducing the risk to an acceptable level, making immediate remediation essential.
High	The severity level is classified as **High** when controls are not in compliance with established control objectives, and gaps can significantly compromise the system if exploited. They should be fixed immediately without any delay. In most cases, successful exploitation leads to a loss of confidentiality, integrity, and availability of data. Compensatory controls are insufficient to mitigate the risk fully, necessitating prompt remediation.
Medium	The severity level is classified as **Medium** when controls are only partially aligned with control objectives. Gaps at this level may allow partial system compromise, enabling an attacker to gain elevated privileges without full control of the system. These gaps pose a significant impact but are less accessible to attackers. Compensatory controls reduce the risk to a degree but do not eliminate it entirely, requiring resolution within a reasonable timeframe.
Low	The severity level is classified as **Low** when controls are in place but leave some residual risk. Gaps at this level present a minor threat, are generally not exploitable across a network, and do not result in full data compromise. Compensatory controls mitigate most of the risk, but some residual risk remains. These issues should be addressed within a defined timeline.

Severity of a particular risk is determined by considering the business impact and corresponding gap/ vulnerability and its associated threat of compromise. So, this is something that the IS Auditor should also consult with the related stakeholders or the business owners. Furthermore, on risk treatment plan it is up to the organization to determine what frequency they follow for gap closure. However, this should be properly defined in the respective document with a reasonable justification of defining the frequency.

2.6 Information System Controls

Information system controls are designed to adhere to the control objectives. Some examples of control objectives are:

To ensure strategic alignment of the business with information technology, accountability, third-party management, compliance with applicable laws and regulations, audits, monitoring, and continuous improvement.

To ensure confidentiality, integrity, and availability of information. It helps to avoid, prevent, identify, mitigate, and remediate risks and vulnerabilities and safeguard organizations' critical assets from potential threats. Its value lies in mitigating risks, ensuring compliance with regulations, protecting data, maintaining business continuity, and enhancing reputation by fostering trust among stakeholders.

There are three types of controls, also referred to as security controls. They are: administrative, technical, and physical. The following section lists down example controls for each of the control categories:

2.6.1 Administrative Control

Refers to management and procedural measures designed to ensure that a business is aligned to its strategic objectives, policies, procedures, guidelines, and regulatory requirements.

- Management rules
- Policies
- Agreements
- Privilege management
- Employee security assessments
- Training initiatives
- Business needs identification
- Monitoring IT strategy and planning
- Organizational structure
- Standards, policies, and processes
- Investment decisions
- Project management
- Vendor management
- Risk management
- Product requirements
- Audit and gap assessment

2.6.2 Physical Control

It refers to anything tangible that is used to prevent or detect unauthorized access to physical areas, systems, or assets.

- Surveillance cameras
- Biometrics
- Identity cards to prevent unauthorized access
- Fencing
- Access control cards
- Locks
- Intrusion sensors

2.6.3 Technical Control

Also known as logical control, it refers to hardware or software mechanisms to protect assets.

- Application-related controls
- Input and output control
- Integrity control
- Process controls
- Network access controls
- Incident management
- Configuration management
- Quality assurance
- Change management
- Logging and auditing

There are other different classifications for types of controls, such as ISO 27001:2022, which classifies controls in four different categories: organizational, people, technical, and physical. Where the organizational and people controls are breakdowns of administrative controls.

Furthermore, based on the functions of security controls, they can be categorized into:

- Directive controls ensure compliance with regulations. These controls can direct human behavior. For example, laws, regulations, policies, etc.
- Detective Control detects a security breach. For instance, a review of logs, CC TV footage, etc.
- Deterrent controls are used to discourage security breaches. Examples include audits, security guards, cameras, and intrusion detection systems.
- Preventive controls aim to prevent incidents from happening. For example, CC TV cameras, segregation of duties, access controls, etc.
- Compensating controls offer alternative security measures. For example, a review before committing work done by a single user can serve as an alternative to requiring two users with segregation of duties. Detective controls are used to identify unauthorized activities.
- Corrective controls mitigate security incidents. For example, virus quarantine, security patching, etc.
- Recovery controls restore systems after an incident. For example, data backup recovery after a ransomware attack.

It is important to understand the concept of security controls. It should also be noted that a single control may fall into one or more categories based on the function it provides.

2.7 Information System Audit

Information Systems (IS) audits play a crucial role in finding gaps in the controls we've discussed before. It's like searching for weak spots in the security system to make sure everything stays safe and protected. The IS audit carefully checks all the rules and plans in place to keep information secure. It looks for any missing or outdated rules that could make it easier for someone to access sensitive data without permission. It's like making sure all the locks on the doors are strong and working properly. Besides looking for gaps in rules and technology, the IS audit also checks if everyone knows what to do in case something goes wrong. By identifying and fixing these gaps, the IS audit helps to ensure that the organization's information system security risks are identified and prioritized for better decision-making. The breadth of the IS audit dictates the level of examination, encompassing the range of IT systems and their operations, IT procedures subject to audit, the geographic spread of IT systems under review, and the duration of audit analysis. The scope of an IS audit is determined by the audit's objectives and the initial risk evaluation of the entity or IT system. During the risk assessment phase, the IS auditor evaluates the policies and protocols governing the entity's overall IT landscape to ensure that adequate controls and enforcement mechanisms are in place. This helps auditors describe the IS audit domains and areas to be included in the scope and determine the depth of audit scrutiny required. The scope of an IS audit, based on the initial risk assessment during planning, can include any or all relevant domains of the audited entity that are relevant to the IS audit objectives:

1. Information Technology, Security & Privacy Governance
2. Information Security Risk Management
3. Compliance
4. Asset Management
5. Human Resources Security
6. Operations Security
7. Endpoint Security
8. Physical and Environmental Security
9. Business Continuity Management
10. Incident Management
11. System Acquisition, Development, and Maintenance
12. Third-Party Service Assessment
13. Access Control
14. Communication Security
15. Cloud Security
16. Mobile Device Management

17. Internet of Thing (IoT) Embedded Systems
18. Configuration and Change Management
19. Cryptography
20. Monitoring and Measurement
21. Application Security
22. Database Security

CHAPTER 3
AUDIT PLANNING & PREPARATION

Audit planning is a crucial part of the audit engagement conducted at the beginning of the audit process. It helps to build a strategy for the audit engagement, emphasizing the procedures for focusing on important areas, identifying risks, and addressing risks to fulfill the audit objectives in an efficient way.

3.1 Appointment and engagement letter

As the first step in audit planning, the auditee provides an appointment letter or purchase order highlighting the high-level work to be done by the IS auditor, including the professional fee for the proposed scope of work.

After receiving the appointment letter, the auditor accepts the engagement by issuing an engagement/ acceptance letter. Both the auditor and auditee should sign the engagement letter to confirm their agreement on the terms of reference.

Along with the engagement letter, the auditor should sign a non-disclosure agreement. Auditors can also incorporate the confidentiality clause into the engagement letter. In that case, there is no compulsion to enter into a separate NDA.

3.1.1 Engagement Letter

An audit engagement letter is an agreement between the client and the auditor that includes the scope of the audit, audit objective, audit criteria, timeline, deliverables, responsibilities of the auditor and the auditee, mode of communication, professional fee, payment terms, a single point of contact for the assignment from the auditor side and the auditee side, and so on. By including these elements, the audit engagement letter establishes clarity, accountability, and mutual expectations, fostering a productive and professional relationship between the auditing firm and the client. The IS Auditor can design the format of the engagement letter, incorporating the above-mentioned sections.

3.1.2 Non-Disclosure Agreement

An NDA (non-disclosure agreement) is a legal contract between the auditing company and the client to keep everything shared during the audit confidential. It helps protect private stuff like trade secrets, financial records, and other sensitive information the auditor might see. The NDA establishes guidelines for the use, sharing, and security of this confidential information. It covers what "confidential information" means, who needs to keep it secret, when it's not required, how long the agreement lasts, and how to handle the information during and after the audit. These rules help lower the risk of misuse and protect both parties' interests and reputations. An NDA makes it clear that people have to keep information secret, adding another layer of safety to the audit process. Taking this step to manage confidentiality helps make the audit more effective and ensures it gets done right and meets its goals.

NON-DISCLOSURE AGREEMENT (NDA)

This Non-Disclosure Agreement (the "Agreement") is entered into on this ___ day of __, 20__, by and between:

ABC Institute Private Limited
Address: [Insert address]
("Disclosing Party")

and

[Audit Firm's Name]
Address: [Insert address]
("Receiving Party")

1. Purpose

The Disclosing Party intends to share certain confidential and proprietary information with the Receiving Party for the purpose of conducting an Information Systems (IS) Audit. The Receiving Party agrees to keep such information confidential and to use it solely for the intended purpose.

2. Definition of Confidential Information

"Confidential Information" includes any non-public information shared by the Disclosing Party related to:

- *IT infrastructure, systems, and applications,*
- *Security policies, controls, and procedures,*
- *Network configurations, passwords, and access codes,*
- *Vulnerabilities, risks, and audit findings,*
- *All documentation, reports, or data generated or provided during the audit.*

3. Obligations of the Receiving Party

The Receiving Party agrees:

- *To keep all Confidential Information in strict confidence and not disclose it to any third party without prior written consent from the Disclosing Party.*
- *To use the Confidential Information solely for the purpose of the IS Audit.*
- *To limit access to the Confidential Information only to its employees, contractors, or agents who need to know the information for the audit and are bound by confidentiality obligations.*

4. Exclusions from Confidentiality

Confidential Information does not include information that:

- *Was publicly available or known to the Receiving Party before disclosure by the Disclosing Party,*
- *Becomes publicly known through no breach of this Agreement by the Receiving Party,*

- *Is independently developed by the Receiving Party without the use of or reference to the Disclosing Party's Confidential Information, or*
- *Is disclosed under legal obligation or governmental request, provided that the Receiving Party promptly notifies the Disclosing Party to allow it an opportunity to seek a protective order.*

5. Duration

This Agreement and the confidentiality obligations shall remain in effect:

- *For a period of [three (3) years] after the conclusion of the IS Audit, or*
- *Until all Confidential Information becomes publicly known through no breach of this Agreement by the Receiving Party, whichever occurs first.*

6. Return or Destruction of Information

Upon completion of the IS Audit or upon the request of the Disclosing Party, the Receiving Party agrees to return or destroy all Confidential Information, including any copies or records, in any form.

7. No License

This Agreement does not grant the Receiving Party any rights, licenses, or ownership in the Disclosing Party's Confidential Information.

8. Remedies

Both parties agree that any breach of this Agreement may result in irreparable harm for which monetary damages may not be sufficient. Therefore, the Disclosing Party is entitled to seek injunctive relief and other equitable remedies in the event of any breach or threatened breach of this Agreement by the Receiving Party.

9. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of [Your Jurisdiction].

10. Entire Agreement

This Agreement represents the entire understanding between the parties regarding the subject matter and supersedes all prior discussions or agreements, written or oral. This Agreement may only be modified in writing and signed by both parties.

IN WITNESS WHEREOF, *the parties have executed this Non-Disclosure Agreement as of the date first written above.*

Signature of Disclosing Party	Signature of Receiving Party
Name	Name
Title	Title
Date	Date

This NDA is structured to protect confidential information disclosed during an IS audit, establishing clear terms for confidentiality, usage, and limitations. Adjust the duration and other specific terms as needed.

The above is a sample of NDA for auditor's reference. It is advised to adjust the NDA sample as per the business need and the need of the client.

3.2 Entry meeting

An entry meeting is a formal meeting conducted to kick off the audit process. It includes all key relevant stakeholders, including the audit team leader, the audit team, and the department heads of the departments to be audited. The audit team leader shares the scope of work, objectives, methodology, relevant approach to work, mode of communication, and point of contact for the audit process. Furthermore, it ensures that all the involved stakeholders are in the same place regarding the scope of work for successfully executing the audit. This meeting also addresses any additional concerns from the department heads.

3.3 Understanding of Auditee business and its environment

The IS auditor should obtain an understanding of the auditee and their business environment, along with applicable IS audit frameworks and guidelines, organizational structure, industry-specific cybersecurity risks, and the and the overall IT infrastructure of the auditee. Examples:

Deployment model, such as on-premises or cloud infrastructure.

Type of operating system (Windows or Linux).

Inherent risk of the auditee.

Nature of auditee businesses like banking, insurance, software development, and cloud services.

Nature of the supply chain, such as sourcing.

An understanding of the applicable areas can be obtained after an interview with the relevant stakeholders, a review of the previous audit report, a review of organizational policies and procedures, etc.

When planning an audit, IS auditors need to understand the company and its processes, as laid out in *ITAF Performance Guideline 1203: Engagement Planning*. Here's what they should focus on:

3.3.1 Business Functions and Environment

It is important for IS auditors to know the business functions and the environment they operate in. This helps them align IT with the company's goals, spot risks, plan audits well, check controls, and suggest improvements. To gather this info, auditors should chat with key people, review documents, watch how things work, attend meetings, and use data analysis techniques. These steps give auditors valuable insights into the business processes, workflows, goals, and challenges, helping them conduct more effective and targeted audits that add real value.

3.3.2 Organizational Structure

Knowing the organization's structure is key for IS auditors. It helps them understand reporting lines, decision-making processes, and who's responsible for what. This helps the auditors identify important stakeholders, assess accountability, check governance mechanisms, and tailor their audit procedures. They should look at organizational charts, policies, and procedures, interview key personnel, and observe how departments interact. This ensures their audit efforts focus on the highest-risk areas important for the organization.

3.3.3 Relevant Laws and Regulations

IS auditors need to understand the laws and regulations that apply to the business. This ensures compliance, reduces legal risks, and protects the company. The auditors should review legal documents, consult legal counsel if needed, and assess the company's compliance programs. Staying updated with legal requirements helps the auditors find gaps, recommend controls, and help the company avoid penalties and damage to its reputation.

3.3.4 Criticality of IT Systems

Knowing which IT systems are crucial, helps IS auditors prioritize their efforts and resources. They should assess the impact and likelihood of risks related to IT systems on business operations, data integrity, confidentiality, and availability. This involves evaluating how these systems support key functions and identifying vulnerabilities. Understanding the criticality of IT systems helps the auditors align their activities with protecting the company's most important assets and strategic goals.

3.3.5 Nature of Systems, Networks, and Applications

IS auditors need to understand the systems, networks, and applications to assess their functionality, security, and compliance with standards and regulations. They should analyze their architecture, design, and configurations to find vulnerabilities and weaknesses. This helps the auditors check controls, assess technology risks, and recommend improvements to ensure data and resource security. This strengthens the IT infrastructure and effectively mitigates risks.

By focusing on these areas, IS auditors can conduct thorough and valuable audits that help improve the company's IT security and overall efficiency.

The following table shows the list of key documents and information required to understand the enterprise:

S.N.	Information Required
1.	Overview of the organization's mission and core objectives
2.	A visual representation of the organizational structure
3.	IT and human resources policies and practices
4.	Relevant legal and regulatory frameworks impacting operations
5.	Inventory of software applications and their specifications
6.	Description of network architecture and key application systems
7.	Roles and responsibilities within the IT department
8.	IT department's involvement in application management

9.	Budget allocation and expenses related to system maintenance
10.	Records of past and ongoing project management endeavors
11.	Hardware inventory and specifications
12.	Software inventory, including in-house development information
13.	Database infrastructure details
14.	Visual representations like data flow diagrams and data dictionaries
15.	Relationship details between database tables and triggers (if applicable)
16.	Interfacing systems and integration protocols
17.	Availability of system, user, and operational manuals
18.	Reports on system performance and optimization efforts
19.	List of authorized users and their access permissions
20.	Test data sets used and outcomes
21.	Security configurations and measures in place
22.	Historical audit reports and their findings
23.	Internal audit reports and actions taken
24.	Feedback from system users and stakeholders
25.	Results of any third-party assessments

On top of a written document, it is always a good practice to ask for an explanation or demo of the related network, system, or application. It offers several advantages:

3.3.6 Clarification of Documentation

Written documents are great, but they might not show the whole picture or all the details. A live demo helps clear up any ambiguities or gaps in the documentation.

3.3.7 Validation of Information

Watching the network, system, or application in action lets IS auditors verify the information in the documents. It ensures the system works as described and there are no discrepancies between what's written and what's real.

3.3.8 Identification of Potential Risks

Seeing the system live might reveal vulnerabilities or risks that aren't obvious in the documents. This helps the auditors spot and address potential security threats more effectively.

3.3.9 Insight into Operational Practices

A demo shows how the system is used in real life. IS auditors can see user interactions, data flows, and how things operate day-to-day, which might not be fully captured in the documents.

3.3.10 Interactive Learning

Demos allow for interactive learning. IS auditors can ask questions, get clarifications, and engage with system administrators or users. This deepens their understanding of the technology and its security implications.

3.3.11 Enhanced Audit Quality

Combining written documents with live demos lets IS auditors conduct a more thorough audit. They can assess the system from different angles, leading to a higher-quality audit report and more actionable recommendations.

3.4 Determining the Components of IS Audit Universe

The scope of an information systems (IS) audit plays a crucial role in defining the parameters within which the audit objectives can be met and drawing effective conclusions. The IS auditor is tasked with creating the IS audit universe, which encompasses key components integral to the organization's information system landscape. The following table assists the auditor in identifying these components:

Items in the IS audit universe	Potential source
Structure of the organization	Organizational charts, divisional, and departmental structures
Laws, regulations, privacy, and other compliance requirements	Legal and regulatory documents, compliance frameworks
Training and awareness	Training plans, human resource developments
Third-party suppliers	Contracts and vendor agreements
Privacy, security, and governance functions	Policies, procedures, and governance frameworks
Audit recommendation follow-ups	Internal audit reports and management recommendations

The list mentioned above is an example, and the auditor should update it as per their needs.

If an organization has its own IS audit function, the audit charter gives a clear mandate to set the scope and carry out the audit. The board of directors or audit committee should approve the audit charter, and it should be reviewed regularly. The scope of an IS audit should meet the audit objectives and draw clear conclusions. The auditor's job is to create the IS audit universe, covering the components mentioned above. As per *General Guidelines 2001*, the board of directors or audit committee should approve an audit charter, and it should include the following sections:

- Aims and goals of the audit function
- Objectives of the audit function and the audit function’s mission statement
- Scope of the audit function
- Work performed by the audit function
- Independence
- Relationship with external audit firms
- Auditee’s expectations
- Auditee requirements
- Abide by professional standards
- Compliance with standards
- Right of access

- Limitations of authority, if any
- Processes to be audited

In the absence of an audit charter, an agreement or engagement letter agreed upon with the auditee serves a similar purpose, outlining the scope, objectives, responsibilities, and expectations for the audit engagement.

3.5 Risk Assessment of IS Audit Universe

Conducting a thorough risk assessment is essential. To conduct a thorough IS audit, it is important to identify and evaluate the risks associated with the areas under review. The objective is to strategically allocate resources, ensuring the IT audit plan is not only comprehensive but also tailored to address the most pressing risks.

As per *ITAF Performance Standard 1201: Risk Assessment in Planning, it* emphasizes the utilization of an appropriate risk assessment approach, blending quantitative and qualitative factors, to craft a well-rounded IT audit plan. This approach serves as the cornerstone for determining priorities and optimizing the allocation of IT audit resources.

As per *ITAF Performance Guidelines 2201: Risk Assessment in Planning*, during the planning phase of individual engagements, the auditor should identify and evaluate risks relevant to the audit scope. These risk assessment outcomes are integral to shaping the audit engagement objectives, ensuring alignment with organizational goals and priorities.

The risk assessment process is multifaceted, considering various factors:

- Insights gained from past audit engagements, reviews, and findings, including any remedial actions undertaken.
- Input from the enterprise's risk assessment process, providing valuable context on overarching risk landscapes.
- Consideration of the likelihood and potential impact of specific risks, quantified in terms of monetary or other value measures.
- The impact of risk.

It's crucial to note that risk assessment should encompass a comprehensive evaluation of all components within the audit universe, factoring in both the probability and consequences of each risk scenario. This holistic approach enables auditors to prioritize their focus and mitigate the risk of erroneous conclusions.

Selecting an appropriate risk assessment methodology is pivotal to ensuring thorough coverage of audit engagements within the designated timeframe. Methodologies may vary, ranging from qualitative assessments based on expert judgment to quantitative calculations yielding numeric risk ratings. Alternatively, a semi-quantitative approach, blending qualitative and quantitative elements, offers a balanced perspective. Recognizing that no single methodology fits all scenarios, IS auditors must tailor their approach based on the enterprise's complexity and the subject(s) under audit scrutiny for system availability, integrity, and confidentiality. Flexibility and adaptability are key, allowing the auditors to navigate the complexities of each audit engagement with precision and efficacy. By

following a rigorous risk assessment process, IS auditors can protect their audit, mitigate risks, and provide valuable insights to stakeholders.

3.6 Audit Plan and Resource Allocation

During audit planning and preparation, the IS auditor should undertake the task of ranking items within the audit universe based on a thorough risk assessment. It is important to validate these rankings with management, as they may possess additional insights or requests for audits that should be incorporated into the current audit universe.

Additionally, the auditor must consider the concept of materiality when planning and executing an audit. As outlined in the ITAF, materiality serves as a pivotal factor in shaping audit expectations and determining audit risk. Notably, the lower the materiality threshold, the more precise the audit expectations become.

In instances where audit risk is high or the materiality threshold is low, the auditor should proactively mitigate risk by either expanding the scope or nature of IT audit tests or by intensifying substantive testing efforts. Conversely, for scenarios where materiality is higher, auditors can mitigate risk by extending the test of controls and/or enhancing substantive testing procedures to obtain further evidence.

The audit team should include individuals with the required competence to conduct IS audit engagements and achieve the desired audit objectives. Necessary knowledge, skills, and competencies for IS audits can be obtained through training, recruitment, and engagement of external resources in alignment with the organization's strategic plan. The IS audit team should collectively possess the capacity to understand the technical aspects of IT-driven information systems, including relevant applications in use, and to navigate the IT infrastructure for the audit process. Furthermore, they should have a comprehensive understanding of applicable rules, regulations, and environmental factors governing the operation of IT-driven information systems. Understanding the mapping of business processes to the programming logic of information systems is also crucial, as is the ability to evaluate the risk of manual overrides and test the effectiveness of application controls. Familiarity with audit methodologies, relevant auditing standards, and guidelines is imperative, as is an understanding of IS management frameworks such as COBIT, ITIL, etc. Additionally, proficiency in IS techniques for collecting audit evidence from automated systems, utilizing IS audit tools for analysis, and accessing IS infrastructure for evidence retention is essential. In cases where IS audits are conducted alongside other audit engagements and seamless integration of the audit team's efforts is critical. This involves comprehensive documentation of tasks, the establishment of information-sharing protocols, and the clear identification of IS audit scope and control objectives.

3.7 Engagement of External Resources

External resources may be engaged, when necessary, with careful consideration given to their training, adherence to professional conduct guidelines, and defined roles and responsibilities. Oversight from in-house team members ensures compliance with audit protocols and service level agreements. It is imperative to establish clear terms of engagement and enforce accountability for external resources involved in IS audit processes. It is the responsibility of the auditor to thoroughly assess and approve the qualifications, relevant experience, independence, and quality control processes of these external

experts before engaging their services. ITAF Performance Standard 1206: Using the Work of Other Experts and ITAF Performance Guidelines 2206: Using the Work of Other Experts serve as invaluable references for auditors in this regard. Some of the key external resources that may be required during an IS Audit process are:

1. Compliance and Regulation Experts: Specialists in areas such as PCI compliance, SWIFT CSP, and Personal Data Protection provide guidance on regulatory requirements and ensure alignment with industry standards.
2. Information Security Standard Experts: Professionals with expertise in frameworks like ISO 27001, NIST, and SOC 2 assist in evaluating adherence to recognized security standards and best practices.
3. Cybersecurity Experts: These experts assess advanced security configurations, perform penetration testing, and manage vulnerability assessments to strengthen the organization's security posture.
4. Incident Response Teams: External incident response specialists offer insights into past incidents and evaluate current response protocols to improve the organization's preparedness.
5. Forensic Investigators: Required for in-depth investigations into data breaches or cybersecurity incidents, forensic experts help validate the effectiveness of corrective controls.
6. Relevant Vendors: Providers of network systems, critical IT infrastructure, cloud infrastructure, and specialized software may be required to clarify technical configurations, patches, or access control mechanisms essential for audit accuracy.

After the required external experts and resources are identified a comprehensive audit plan is prepared. In this plan, the auditor should schedule the audit and allocate time and resources as required to execute the audit plan effectively. It is essential for the audit plan to seamlessly integrate with the team engagement for audit planning and preparation. By synchronizing resource allocation with team engagement, auditors can ensure optimal utilization of resources and alignment with audit objectives.

CHAPTER 4
AUDIT EXECUTION

4.1 Audit Program

IS auditors should develop and document an audit program that describes the step-by-step procedures and instructions to be used to complete the audit. The audit program is the set of procedures performed to obtain sufficient and appropriate evidence. The auditor should develop the audit program or audit completion checklists as required.

Once the audit planning is completed, the auditor should have enough information to identify and select the audit approach and start developing the audit program. The following are the activities performed to develop an audit program:

- Identify and obtain departmental policies, standards, and guidelines for review.
- Identify any regulatory compliance requirements.
- Identify individuals for the interview.
- Identify methods to perform evaluations.
- Develop test scripts, etc.

4.2 Field Work

The fieldwork is where the auditor gathers evidence and conducts detailed testing to evaluate the effectiveness of controls. This phase involves reviewing documentation, interviewing stakeholders, and performing technical tests. Following are the activities to be performed during the field work phase:

1. **Documentation Review**: To ensure an organization's adherence to established standards, examining its policies, procedures, and past audit reports is a fundamental step in the IS audit process. This process involves a thorough review of the documentation and practices that define the organization’s control environment. Examining policies, procedures, and past audit reports allows auditors to verify that the organization’s control environment is compliant with industry standards and regulatory requirements. This comprehensive review provides a foundation for evaluating whether the organization’s information systems are secure, reliable, and resilient. Additionally, it helps identify any deviations from best practices and potential areas for improvement, enabling the organization to enhance its overall risk management strategy.
2. **Testing Controls**: Testing various controls is a key component of the IS audit process, as it helps determine whether an organization’s information systems are secure, reliable, and compliant with industry standards. Each control addresses specific aspects of the organization’s risk management and operational resilience. Details on control domains are explained in section [4.5].
3. **Interviews with Key Stakeholders**: Engaging with IT personnel, business users, and system owners is essential in the IS audit process as it provides critical insights into the organization’s operational processes, workflows, and potential vulnerabilities within the system. By interacting

directly with these key stakeholders, auditors can gain a comprehensive understanding of how systems are used daily, uncover areas where users might bypass controls, and identify any misalignments between documented procedures and actual practices. These discussions also help reveal knowledge gaps or dependencies on specific individuals, which may increase operational risks. Additionally, stakeholders often provide valuable context for audit findings, helping auditors assess the real-world impact of any identified weaknesses and enabling more tailored recommendations to strengthen the organization's overall security and efficiency.

4. **Technical Testing**: Performing vulnerability assessments, penetration testing, or other technical evaluations is a crucial step in identifying and addressing potential security weaknesses within an organization's information systems. A vulnerability assessment systematically scans systems and networks to uncover flaws, misconfigurations, or outdated software that may expose the organization to cyber threats. Penetration testing, on the other hand, involves simulating real-world attacks to exploit identified vulnerabilities, providing a more in-depth understanding of how an attacker might breach the system and gain unauthorized access to sensitive data. These technical evaluations go beyond surface-level checks, allowing auditors to measure the robustness of security controls, identify areas for improvement, and prioritize remediation efforts based on the severity and exploitability of vulnerabilities. By conducting these assessments, auditors help the organization strengthen its defenses, reduce the risk of cyber incidents, and enhance its overall security posture.

5. **Evidence Collection**: Collecting evidence through observations, system walkthroughs, and data analysis is a fundamental part of the IS audit process, providing auditors with concrete insights into the organization's information systems and control environment. Observations allow auditors to witness operations in real time, identifying any discrepancies between documented procedures and actual practices. System walkthroughs provide a step-by-step understanding of how users interact with systems, uncovering potential points of failure, security gaps, or areas where controls may be bypassed. Data analysis, meanwhile, enables auditors to examine logs, transaction records, and other digital footprints to identify patterns, anomalies, or unauthorized activities that might indicate underlying issues. Together, these methods provide a comprehensive body of evidence that supports the audit findings, ensuring that recommendations are well-founded and targeted toward areas that will genuinely enhance the organization's security, compliance, and operational efficiency.

4.3 Sampling

If the examination of all the information is impractical during the audit, valid conclusions can be reached using audit sampling. Sampling can be statistical or non-statistical. Nonstatistical sampling is used by auditors who want to use their own experience, knowledge, and professional judgment to determine a sample. This method may likely reflect human bias. Therefore, results should not be extrapolated over the population because the sample is unlikely to be representative of the entire population. Non-statistical sampling may be used when results are needed quickly to confirm a proposition, but it should not be used to draw mathematically constructed conclusions regarding the entire population.

But statistical sampling uses mathematical techniques to draw conclusions. So, a conclusion regarding an entire population can be reached using statistical sampling.

Sampling should not be used in some instances. For example, sampling should not be used for tests of controls if there is no evidence of performance, such as appropriate segregation of duties. In such cases, a complete review is required, and the effectiveness of controls cannot be determined by samples.

When designing the size and structure of an audit sample, the IS auditor should consider the specific IS audit objectives, the audit procedures that are most likely to achieve those objectives, the nature of the population, the nature of the control (e.g., manual or automated), relevant subgroups within the population, and the sampling and selection methods. In addition, when audit sampling is appropriate, consideration should be given to the nature of the evidence sought, possible error conditions, and possible root causes.

The purpose of the sample can be:

- Compliance testing/test of controls: An audit procedure designed to obtain audit evidence on the effectiveness of the controls and their operation. Examples can be program change control procedures, review of logs, etc.
- Substantive testing/test of details: An audit procedure designed to obtain audit evidence on the completeness, accuracy, or existence of activities or transactions during the audit period. An example can be the re-performance of a complex calculation (e.g., interest) on a sample of accounts.

When determining sample size, the IS auditor should consider the sampling risk, the amount of error that is acceptable, and the extent to which errors are expected.

After performing the audit procedures aligned with the IT audit objective on each sample item, the auditor should analyze any possible errors detected in the sample to determine if they are actual errors. For possible errors that are determined to be actual errors, the nature and cause of the errors should be identified. Also, the errors should be projected as appropriate to the population, but only if a statistically based sampling method is used.

It is recommended to refer to ITAF Companion Performance Guidelines 2208: Information Technology Audit Sampling.

4.4 Evidence Gathering

IS auditors should obtain sufficient and appropriate evidence to draw reasonable conclusions. Applying professional skepticism, the auditor should evaluate the sufficiency of the evidence obtained to support conclusions.

When planning and performing an engagement, auditors should consider the types of evidence to be gathered, its use to meet engagement objectives, and its varying levels of reliability.

The various types of evidence that practitioners should consider using include the following:

4.4.1 Review of processes and verification of tangible items

Observed processes and the existence of physical items can include observations of activities, property, and IT functions, such as:

- A SIEM collecting log data

- A backup system

4.4.2 Documented evidence

Evidence documented on paper or other media can include:

- Written policies and procedures
- Results of data extractions
- Records of transactions
- Program listings
- Relevant business documents and records
- External confirmation from third parties

4.4.3 Representations (management statements)

Representations (written and verbal) can include:

Official documents, management confirmation of properly functional internal controls, and new system implementation plans.

Verbal representations of things such as how a process works or management plans follow up on actions related to the security awareness program.

If evidence obtained in the form of verbal representations is critical to the audit finding or conclusion, the auditor should consider obtaining confirmation of the representations, either in writing or electronically (such as through email). The auditor should also consider alternative evidence to corroborate such representations to ensure their reliability.

4.4.4 Analysis

After the field work, analysis is another key aspect in IS Audit process. Analysis is the process through which the auditor determines the gaps and provides recommendations. Following are the key activities to be performed during the analysis phase:

1. Risk Assessment: Evaluate the risks associated with identified weaknesses and potential impacts on the organization.
2. Determine Control Effectiveness: Assess whether the existing controls effectively mitigate the identified risks.
3. Identify Areas of Non-Compliance: Highlight instances where systems or processes deviate from regulatory or internal standards.
4. Formulate Recommendations: Develop actionable recommendations to address identified vulnerabilities and enhance control measures.

The results produced through the analysis of information can also be used as evidence. Analysis may be done through comparisons, simulations, calculations, and reasoning. Examples include:

- Benchmarking IT performance against other enterprises or past periods.

- Comparing the rate of errors, login failures, incidents, etc. between different timeframes, domains, and physical locations.
- Re-performance of processes or controls, for example, review of access logs.

Procedures used to gather evidence vary depending on the characteristics of the information system being audited, the timing of the audit, the scope and objectives of the audit, and professional judgment. The following procedures can be considered:

- Inquiry and Confirmation
- Observation
- Inspection
- Analytical Procedures
- Recalculation
- Re-performance

When gathering evidence, the auditor should consider the independence and qualifications of the entity providing the evidence.

Further, the auditor may be able to conduct an IS audit remotely. In such cases, the auditor should determine feasibility before the audit starts so that the engagement objectives are met. Common issues that may arise in gathering evidence during a remote audit include:

- Organizational policy restrictions prohibit the auditor or auditee from installing software not authorized by each other's organization.
- Having difficulty with screen sharing on specific IT platforms or applications.
- Limited access to items of interest in the IT environment is due to the systems hosted on third-party platforms.

So, effective planning is crucial for comprehending the total effort needed to achieve audit objectives in a remote IS audit. The auditor can refer to *ITAF Performance Standard 1205: Evidence* and *ITAF Performance Guidelines 2205: Evidence*.

4.5 Audit Domains

Before getting into the detailed checklists for each of the 22 domains outlined in the annexure, it is imperative to underscore the significance of understanding the scope of the audit. The scope delineates the extent of scrutiny and the areas to be covered during the audit process. As such, it is crucial for the IS auditor to fully understand the controls related to specific domains to effectively perform the audit. However, given the complexity and specialized nature of certain domains, it may be necessary for the auditor to seek assistance from external experts to ensure a thorough evaluation. This overview of the 22 domains aims to provide a brief yet informative glimpse into each domain, offering valuable insights to guide the audit process and facilitate informed decision-making. The following section discusses various domains included in the IS audit process, including the high-level risk associated with each domain.

4.5.1 IT Governance

IT governance is the governance practice (derived from ISO 38500) through which an organization controls, manages, and guides the effective use of information technology. IT governance is a system by which an organization's IT and information security activities are directed and controlled through:

- Policies and procedures
- Organization structure
- Delegation of authority by defining roles and responsibilities
- Performance measurement
- IT security governance

The management of IT security is different from the governance of IT security. It defines responsibilities and procedures for the executive management in order to provide a strategic direction to achieve organizational goals, manage risks, and optimize resource usage. An effective information security governance system should consider the following:

- Security as a part of business strategy and risk management
- System resiliency and incident response
- Data protection and privacy
- Adoption of new technologies
- Collaboration and communication between stakeholders

An organization with good information security governance practices will have a robust information system security strategy supported by management and focused on continuous improvement.

Enterprises generally establish governance through steering and strategy committees. The strategy committee advises the board of directors on strategies to enable better IT support of the organization's overall strategy and objectives, while the steering committee oversees the execution of strategies chosen by the board of directors.

ISACA's Control Objectives for Information and Related Technology (COBIT) framework is widely used by organizations for establishing and maintaining IT governance. This framework emphasizes the difference between governance and management.

Information security governance comprises activities that establish key roles and responsibilities, identify and treat risks to key assets, and measure key security processes.

Depending on the organization's structure and business purpose, information security governance may be included in IT governance.

Privacy governance involves established activities focused on ensuring an organization's adherence to fundamental privacy principles and outcomes, providing management with a clear understanding of the state of the organization's privacy program, its current risks, its activities, and its alignment with business objectives.

The processes supporting these principles and outcomes include privacy policy, data governance, compliance, risk management, and information security.

Privacy governance involves the structured management of personal information within an organization, ensuring adherence to fundamental privacy principles and legal requirements. It encompasses the establishment of policies, processes, and controls to safeguard personal data and ensure transparency, accountability, and compliance.

Key components of privacy governance include:

- Privacy Policies: Clearly defined rules on how personal information is collected, used, stored, and protected.
- Data Governance: Processes for managing and protecting personal data throughout its lifecycle, including classification, access controls, and retention policies.
- Compliance: ensuring adherence to relevant privacy laws, regulations, and standards, such as GDPR, CCPA, and ISO/IEC 27701.
- Risk Management: Identifying and mitigating privacy risks associated with personal data processing.
- Information Security: Implementing security measures to prevent unauthorized access, disclosure, alteration, or destruction of personal data.

Considerations related to data privacy include:

- International Standards: Aligning privacy practices with global standards to ensure legal compliance.
- Data Minimization: Collecting and retaining only necessary personal data to reduce privacy risks.
- Transparency: providing clear and understandable information to individuals about data processing practices.
- Consent: obtaining explicit consent from individuals before collecting or processing their personal data.
- Data Subject Rights: Respecting individuals' rights regarding their personal data, including access, rectification, and deletion.
- Data Breach Response: Having procedures in place to respond effectively to data breaches and notify affected parties as required.

Risks

1. Lacking management commitment.
2. Business strategy not aligned with IT, security, and privacy strategy or missing IT, security, and privacy strategy.
3. Lack of understanding of information system security and privacy.
4. Undefined roles and responsibilities.
5. Undefined policies and procedures.

4.5.2 Information Security Risk Management

Risk is the effect of uncertainty on objectives. It can also be defined as the potential that a given threat will exploit the vulnerabilities of an information asset and cause harm to the organization. Generally, risk can be calculated as follows:

Risk = P x I

Where,

P = probability that a threat may exploit vulnerabilities (T x V)

I = Impact of threats exploiting vulnerabilities

T = Threat

V = vulnerability

Quantitative, qualitative, or semi-quantitative methods may be used for risk assessment.

Overall IT risks may be broadly classified in terms of the following:

- Benefit/value Enablement risk
- IT project delivery risk
- IT operations and service delivery risk
- Information security risk

Risks may have an adverse impact on the achievement of the objectives of the enterprise. So, the risk efforts should be integrated into the enterprise for effective benefit realization and resource optimization. Different frameworks and standards can be used as references for understanding and evaluating risk management practices, such as ISO 31000:2018, Risk Management Principles and Guidelines, ISO 27005:2018, Information Technology, Security Techniques, Information Security Risk Management, the NIST Risk Management Framework (RMF), the NIST SP 800-30 Guide for Conducting Risk Assessments, etc.

Information security risk management is the process of assessing, prioritizing, and addressing the risks associated with the use of information technology. A risk management process includes the following steps:

- Identification of assets: This is the first step to identify and classify all in-scope assets.
- Risk assessment: It identifies the threat, vulnerability and impact for each asset.
- Risk prioritization: It prioritizes the risks based on the criticality.
- Risk mitigation: It implements strategies and controls to address the risks based on priority.
- Monitoring: Risk management is a continuous process, it continuously monitors the vulnerabilities, threats, associated risks as well as the risk treat treatment strategy.

Risks

1. Undefined risk management policies and procedures.

2. Undefined risk register.

2. Missing risk prioritization, closure plan, and practice.

4.5.3 Compliance

Compliance requires an organization to take the necessary steps to meet internal security and regulatory requirements. Compliance is a measure for organizations to prioritize and follow best practices for information system security. Through compliance, organizations can prevent breaches of legal, statutory, regulatory, or contractual obligations. Therefore, an organization should identify applicable legislation, contractual requirements, and procedures to ensure compliance with the applicable regulatory requirements (NRB, NTA, and insurance).

Risks

1. Organizational policy is not aligned with national and industry regulations.
2. Missing awareness related to applicable compliance and regulations.

4.5.4 Assets Management

An organization should define practices for the identification and inventorying of information assets involved in the usage, maintenance, and disposal of information assets to protect information used by the organization and achieve efficient and effective service delivery. This can be done through:

- Maintaining an inventory of assets with proper labeling and ownership.
- Formulating rules for acceptable use.
- Classifying information in terms of legal requirements, value, and criticality.

Risks

1. Undefined asset management policy, asset/information classification policy.
2. Undefined asset movement policy and procedure.
3. Undefined asset disposal policy and procedure.
4. Missing inventory of assets.

4.5.5 Human Resource Security

Since humans are the weakest link in the overall security chain, it is crucial to consider human security. It is important to ensure that related stakeholders (employees and third-party vendors) understand their responsibilities and are suitable for their roles. The goal of HR security is to protect the organization's interests by effectively applying the below-mentioned controls:

- Employee Screening
- Information security education, training, and awareness
- Termination or change in employment responsibility

Risks

1. Undefined roles and responsibilities.
2. Undefined security and confidentiality clauses in contracts.
3. Missing employee background verification.
4. Missing employee termination policy and process, including exit interview, revoking credentials, handling of assets, etc.
5. Lack of employee awareness regarding information security policy and responsibilities.

4.5.6 Operations Security

Operational security, known as OPSEC, is a strategic approach employed by organizations to safeguard confidential information from unauthorized access. It involves recognizing seemingly harmless actions that could inadvertently expose sensitive data to potential threats. OPSEC prompts IT and security professionals to evaluate their systems and operations through the lens of potential adversaries, employing analytical techniques and implementing security protocols and best practices. Generally, the following domains are considered in this section, but are not limited to:

- Operational procedures and responsibilities: A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event. *Source: NIST Glossary.*
- Controls against malware: Protection mechanisms should include scanning, blocking, and/or quarantine at network entry and exit points, email gateways, servers, and end systems. The enterprise should update malicious code protection mechanisms as per its change and configuration management policies and procedures. Enterprise personnel should be trained in the effective use of anti-malware software.
- Information Backup: To protect against loss of data.
- Logging and monitoring: To record events and generate evidence.
- Technical vulnerability management: The vulnerability management process of the enterprise should help identify exploitable weaknesses (which is a susceptibility or flaw in a system that an attacker can access and exploit to compromise system security) in critical systems and technologies, as well as conditions that allow for human error and accidents in critical functions, supporting processes, and information assets.

Risks

1. Gaps in access control policies and procedures.
2. Missing incident response plan.
3. There is no patch management process.
4. Missing security monitoring mechanism.
5. Missing awareness and training programs.

4.5.7 Endpoint Security

Endpoint security refers to the approach and set of technologies designed to protect individual computing devices (endpoints), such as desktops, laptops, servers, and mobile devices, from various cybersecurity threats. The primary objective of endpoint security is to safeguard these endpoints from malware, ransomware, phishing attacks, unauthorized access, and other security risks. Some of the key areas of endpoint security are:

- Antivirus and Antimalware: Software that detects, blocks, and removes malicious software (malware) from endpoints.
- Firewall Management: Controls incoming and outgoing network traffic based on predetermined security rules, preventing unauthorized access to endpoints.
- Intrusion Detection and Prevention Systems (IDPS) monitor network traffic for suspicious activities or patterns indicative of an attack and prevent or mitigate threats.
- Encryption: It protects sensitive data stored on endpoints or transmitted over networks by converting it into ciphertext, making it unreadable to unauthorized users.
- Endpoint Detection and Response (EDR): advanced threat detection and response capabilities that continuously monitor and analyze endpoint activities to identify and respond to security incidents in real-time.
- Patch Management: Ensures that endpoints are up to date with the latest security patches and updates to address known vulnerabilities.
- Device Control: Manages and controls access to peripheral devices (such as USB drives, printers, and external storage) connected to endpoints to prevent data leakage or unauthorized access.
- Application Whitelisting and Blacklisting: Controls which applications can run on endpoints based on predefined lists, reducing the risk of malware infections and unauthorized software installations.

Risks

1. Missing end-point security policy.
2. End-point security solutions are not used at end-points (workstations and servers).
3. Full disk encryption is not done at end-points (workstations and servers).
4. Missing patches on end points.

4.5.8 Physical and environmental security

Information and other related assets should be protected by clearly defined security perimeters. To stop unwanted physical access, harm, and interference with the organization's data and other related assets. Enterprise should ensure the following:

- Information processing facilities and areas containing sensitive and/or critical information are protected by defined security perimeters,
- Access to secure areas is restricted to authorized personnel only by means of the proper entry controls,

- Reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, critical computing equipment is situated and safeguarded. Critical computing equipment should be physically protected with features like water damage protection, fire suppression systems, temperature and humidity controls, and emergency power and lighting,
- Wireless access points, power cables, and telecommunications cabling related to critical systems should be protected from tampering and damage,
- Equipment is properly maintained to ensure its continuous availability and integrity.

Risks

1. Missing physical security policy.
2. Missing controls such as preventive (locks), detective (CC TV), deterrent (fences), etc., as applicable.
3. Missing access to the to the right review process.
4. Missing policies and procedures for visitors' access.
5. Missing appropriate controls against threats such as fire, flood, etc.
6. Missing power backup.
7. Missing policies and procedures to prevent theft and loss of office assets such as devices, workstations, servers, and other equipment.
8. Missing inventory of office assets.

4.5.9 Business Continuity Management

BCP is the preparedness plan of an organization in case of disaster; it includes policies, procedures, guidelines, and controls to ensure continuity of critical business processes and functions at an agreed level and limit the impact of the disaster on people, processes, and infrastructure. Furthermore, through BCP, an organization can minimize the operational, financial, reputational, and legal consequences that may be caused by a disaster.

BCM includes IT Availability Management (Capacity Monitoring and Planning), IT Continuity Management (Data Backup, Disaster Recovery, IT Continuity Planning, Outsourced Relationship management, Testing of BCP, and Review of BCP).

BCP aims to continue the operation or business in the event of a disaster, whereas the disaster recovery plan (DRP) covers technical aspects and aims to recover the information system in the event of a disaster.

Further, information security continuity shall be embedded in the organization's business continuity management systems.

Organizations can use NIST SP 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems for their business continuity planning.

Risks

1. Missing BCP, DRP, and Business Impact Assessment (BIA).

2. BCP and DRP plans are not tested.
3. Undefined RTO, RPO.
4. Business-critical processes, functions, and assets are not defined.
5. Users do not have a clear understanding of their roles during disasters.
6. Missing backup and recovery strategy, system and testing.

4.5.10 Incident Management

Incident management is the process of managing incidents within an organization within a minimized response time to contain and recover from the incident. An incident can be anything from a ransomware attack to a system crash, data exfiltration, or power failure. An effective incident management process should include the following:

- Establishing management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.
- Reporting information security events through appropriate management channels
- Using knowledge gained from analyzing and resolving information security incidents to reduce the likelihood or impact of future incidents.
- Define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

Risks

1. Missing information security incident management policy, process, criteria, classification mechanism, and severity matrix.
2. Lack of responsibility and awareness among employees and related stakeholders.
3. There is no incident response team.
4. There is no recorded evidence of past incidents.

4.5.11 System Acquisition, Development, and Maintenance

Secure SLDC is required to ensure that information security is an integral part of information systems across their entire lifecycle.

Technology standards (infrastructure standards, application security standards, availability standards) and risk management of new technology should be considered during the acquisition and development of information systems. Generally, the following aspects should be considered:

- Software development lifecycle (SDLC): To ensure that all SDLC steps are followed properly, from requirement identification to testing, implementation, and maintenance.
- Secure software development lifecycle: To ensure that security is embedded throughout the software development life cycle, including provision for continuous monitoring.
- Protection of test data: To ensure the protection of data used for testing.

Risks

1. Missing a secure software development lifecycle.
2. Missing threat modeling process.
3. Missing requirement analysis both in the development and procurement processes.
4. Security control tests are not planned and conducted.

4.5.12 Third Party Service Management

As organizations expands its business, there is an increasing reliance on external service providers as partners in achieving the growth targets and as effective cost alternatives. Below aspects relating to outsourcing need to be considered:

- Document and agree upon information security measures with suppliers to mitigate risks related to their access to organizational assets.
- Include information security requirements as a part of the contract process.
- Conduct independent security and privacy risk assessments at regular intervals.

Risks

1. Missing policies and procedures for third party risk management.
2. Missing service level and non-disclosure agreement.
3. Missing security controls to manage third-party access control.
4. Missing third-party risk assessment.

4.5.13 Access Control

Access control provides a set of practices for accessing an organization's information and information systems (operating systems, applications, databases, network equipment, and others). Access controls pertaining to an organization's information and information systems shall be based on the principles of "User Authorization" and "Accountability" and support the security concepts of "least privilege access", "need-to-know", "segregation of duties", and "individual accountability". Enterprise should:

- Limit access to information and information processing facilities.
- Prevent unauthorized access.
- Ensure users act responsibly and are accountable for securing authentication details.
- Prevent unauthorized access to systems and applications.

Risks

1. Missing proper access control policy and procedure.
2. Gaps and vulnerabilities in access control of the network, endpoints, devices, servers, cloud, remote network, and physical environment.

3. Undefined process and controls for granting and revoking access.
4. Not following practices such as the principle of least privilege and segregation of duties.
5. Missing session lockout controls, multi-factor authentication, etc.

4.5.14 Network and Communication Security

Network and communications security refers to the protection of network and communication infrastructure, the information transmitted, and the associated users. It is the backbone of any information system infrastructure. It ensures a secure and reliable network, including any network and communication protocol such as email, messaging, file transfers, remote connections, etc.

Risks

1. Missing network and email security policies.
2. Missing network diagram.
3. Missing network segregation as required by the business function.
4. Missing HA for network devices (access point, firewall, VPN, router, switch).
5. Missing appropriate usage of specific technology as per business and security needs. For example, not using a VPN in cases of remote access.
6. Missing network monitoring.
7. Weak access control.
8. Missing email encryption.
9. Missing multifactor authentication.
10. Missing spam filtering.
11. Weak password policy.

4.5.15 Cloud Security

While considering security in a cloud environment, the cloud service provider is responsible for implementing and configuring some aspects of the computing environment, while the customers are responsible for other aspects of the environment. This approach to security responsibility is known as the shared responsibility model, and it determines the scope of security applicable to each party. The following table shows an example of a shared responsibility model:

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance	Customer	Customer	Customer	Customer
Client access endpoints	Customer	Customer	Customer	Customer
Identity and access management	Customer	Customer	Customer	Customer
Application Security	Customer	Customer	Shared	Provider
Network Security	Customer	Customer	Shared	Provider
Operating System Security	Customer	Customer	Provider	Provider
Physical Security	Customer	Provider	Provider	Provider

Cloud computing risks by computing models:

- Infrastructure as a Service (IaaS): In this model, the customer will have the most control over their resources.
- Platform as a Service (PaaS): In this model, service providers provide customers with a platform where they can run their own application code without worrying about server configuration. This is the middle ground between IaaS and SaaS.
- Software as a Service (SaaS): In the SaaS model, the public cloud provider delivers an entire application to its customers. Customers don't need to worry about processing, storage, networking, or any of the infrastructure details of the cloud service. Very often, these services are accessed through a web browser, so very little, if any, configuration is required on the customer's end. Common examples include email services, Microsoft Office 365, Dropbox, etc. All the risks inherent in the PaaS and IaaS models remain in the software as a service (SaaS) environment, along with these additional risks.

Risks

1. Third-party risk due to limited control leading to a security breach if the vendor has a security breach.
2. Security misconfigurations (default accounts, credentials, improper logging, exposed access keys, weak passwords, open ports and services, encryption, insecure API, etc.)
3. Compliance and regulations for the business might not be addressed by the service provider.
4. Limited visibility of the underlying layers.
5. Risks due to application layer vulnerabilities due to insecure software development practices.

The level of risk can vary based on the type of service and nature of the business. IS auditors are advised to understand the business model and nature of cloud services to determine the applicable risks.

4.5.16 Mobile Device Management

An organization can deploy the use of mobile devices through the Bring Your Own Device (BYOD) policy. This policy allows employees to bring their own personal mobile devices to work and may allow them to use those devices to connect to business resources and/or the internet through the company network. Instead of BYOD, some organizations may also implement the concept of corporate-owned, personally enabled, i.e., organization that purchase devices and provide them to employees.

The organization needs to ensure sensitive and critical data of the organization that is accessible by the employees on their mobile devices is protected against unauthorized access and prevents unauthorized information disclosure. It should also consider the separation of private and business use of the devices, including using software to support such separation and protect business data on a private device.

Risks

1. Missing mobile device management policy.

2. Missing encryption.
3. Loss of device.
4. Missing malware protection.
5. Missing patches and updates.
6. Installation of unwanted applications; missing web filtering mechanism.

4.5.17 Internet of Things (IoTs) Embedded Systems

IoT embedded systems are computer systems and embedded systems that enable them to communicate over the network. They consist of microcontrollers, communication protocols, and sensors used for data collection, processing, and transmission. IoT embedded systems are used in office automation (for air quality, temperature, humidity, smart mirrors), data center automation, digital hoarding boards, etc.

IoT embedded systems carry a high degree of security risk due to a lack of proper security controls.

For securing IoT systems, it is advised to refer to the OWASP IoT Top 10, which can be used for hardening IoT systems.

1. Missing policies for procuring, maintaining, and securing IoT systems.
2. Procurement from an untrusted vendor.
3. Interface access from a public network.
4. Weak authentication and authorization.
5. Application and firmware vulnerabilities.
6. Lack of security updates.
7. Physical access and theft.

4.5.18 Configuration and Change Management

Change management is a continuous process of controlling and approving changes to information system assets that support the critical services of an organization. The change management process includes additions, removals, and changes to assets.

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. These errors can cause operational failures, leading to financial, reputational, and legal risks. Having a configuration and change management process to protect against these risks is vital to the organization's overall security posture.

This mainly involves the following steps:

- Create a plan or procedure for configuration and change management (baseline configuration).
- Identify configurable items out of total assets and define and create an inventory of baseline configurations.

- Implement configuration changes as per the defined procedure, if changes are required, and update the configuration inventory.
- Monitor configuration changes to ensure that changes are identified, proposed, reviewed, and tested prior to implementation.

Risks

1. Missing configuration management and change management policies.
2. The change management process was not followed properly.
3. Inventory of assets and processes applicable for configuration management and change management processes.
4. Default configuration has not been changed.
5. Missing configuration backup of critical assets.

4.5.19 Cryptography

It is a crucial instrument for computer security, pertaining to methods of transferring and storing data that shield it from unwanted access or manipulation. Cryptographic controls define the desired practices for the use of cryptographic controls for the protection of confidentiality and integrity of an organization's organizational assets.

Cryptography is vital for securing information through encryption methods like symmetric and asymmetric-key encryption. Organizations establish cryptography policies to guide encryption practices and ensure compliance with standards. Key management is essential for effective encryption, encompassing processes for secure key generation, exchange, and storage. Strong cryptography and key management practices are crucial for protecting digital assets and maintaining trust in digital transactions.

Risks

1. There is a missing policy regarding the use of cryptographic controls.
2. Missing appropriate cryptographic controls for data at rest and data in motion, including mobile devices.
3. Missing key management processes, including secure disposal of cryptographic materials.
4. Digital signatures are not used for verifying the authenticity and integrity of sensitive communication, e.g., email, financial, legal, and other sensitive documents.

4.5.20 Monitoring and Measurement

Monitoring is watch and detect, is less complex, and can provide a quicker alert when things become different than expected, while measurement (value) can provide more detailed information about the situation and how things should be handled.

The organization should have a performance monitoring and measuring system for IT functions and report it to an appropriate level of management.

The organization should also continually improve the suitability, adequacy, and effectiveness of the information security management system with the help of monitoring and measurement.

The following aspects should be established to ensure proper monitoring and measurement:

- What needs to be monitored? Examples of e-commerce systems' availability, accounting data integrity, and special access rights
- Which methods may be used for monitoring? Examples: manual, mechanical, software, etc.
- When monitoring must be done: Different needs require different monitoring timings, and the organization must consider this, including periodicity. Example: An application can have monitoring points at data input, during data processing, or at data output.
- When monitoring results must be analyzed and evaluated: To add value to the business, the monitoring results must be considered in decisions and actions at the proper time.
- Who must analyze and evaluate monitoring results? As important as when the data is analyzed, it is also important who does this. In general, the operational level should perform analysis (e.g., technicians and administrators), while management staff perform evaluations.

Risks

1. Missing a continuous monitoring strategy at the system and organizational levels.
2. Missing monitoring of vital or critical assets and processes.
3. Undefined KPIs for monitoring.
4. Missing independent assessment of monitoring controls.
5. Missing correlation and alerting capacity to detect any suspicious activities.
6. Missing capacity for threat hunting, threat intelligence, and incident investigation.

4.5.21 Application Security

Application security is another critical component of overall information security, focusing on protecting software applications from vulnerabilities and threats that could compromise the confidentiality, integrity, and availability of data and systems. In the case of application development, adopting a secure development lifecycle (SSDLC) is essential for building secure applications from the ground up. This involves integrating security into every phase of the software development process, from design and coding to testing and deployment.

Risks

1. Missing application security policies.
2. Missing a secure supply chain management process for applications and underlying libraries.
3. Weak input, output, integrity, and processing controls.
4. Insecure authentication and authorization process.
5. Missing controls to protect against injection attacks.
6. Weak of cryptographic controls.

7. Others have risks as per the OWASP top 10 vulnerabilities.
8. application audit and vulnerability assessment process.
9. Missing secure development practices, including secure design, threat modeling, code review, security testing, configuration management, monitoring, etc.

4.5.22 Database Security

Database security is critical for overall information security, focusing on the protection of data stored within databases from unauthorized access or manipulation. Effective database security measures are essential to safeguarding the confidentiality, integrity, and availability of organizational data assets.

Encryption Practices: Encryption is fundamental to securing information within databases. Organizations establish encryption policies to govern the implementation and usage of encryption technologies, ensuring adherence to industry standards and regulatory requirements. This includes defining encryption algorithms, key lengths, and encryption methods suitable for different types of data and applications.

Key Management: Key management is central to the effectiveness of encryption practices within database security. It encompasses the secure generation, distribution, exchange, storage, and disposal of cryptographic keys used for encryption and decryption processes. Proper key management practices ensure the confidentiality and integrity of encrypted data and mitigate the risk of unauthorized access or key compromise.

Ensuring Compliance: Strong cryptographic controls and key management practices are essential for organizations to maintain compliance with regulatory mandates and industry standards governing data protection. By implementing robust cryptographic controls and adhering to established key management protocols, organizations can demonstrate due diligence in safeguarding digital assets and protecting sensitive information from unauthorized disclosure or misuse.

Risks

1. Weak security restrictions (access control, permission, password control) to access and make changes to databases.
2. Missing backup and recovery process and implementation both for the database and its configuration.
3. Missing vulnerability assessment and penetration testing practices.
4. Disabled auditing.

4.6 Documentation of Evidence

IS auditors should document the evidence obtained and ensure that documentation is retained and available during a predefined period in a format that complies with enterprise policies and relevant professional standards, laws, and regulations.

Furthermore, IS auditors should also ensure that documentation of evidence is protected from unauthorized access, disclosure, or modification throughout its preparation and retention and should dispose of evidence documentation at the end of the established retention period.

4.7 Other Control Frameworks and Standards

Various national and international information security governance and control frameworks, standards, and regulations exist to evaluate, enact, and improve the security posture and risk management strategies of an organization in alignment with the prevailing threat landscape.

Such frameworks and standards can be used by an IS auditor for gap analysis and maturity assessment to minimize security risks in the organization. An IS auditor may refer to each of these frameworks (but not be limited to) for their reference:

- NIST Cybersecurity Framework 2.0
- NIST SP 800-53a (Security and Privacy Controls in Information Systems and Organizations)
- NIST SP 800-53 (Security and privacy controls for information systems and organizations)
- ISO/IEC 27001:2022 (Information security management systems)
- Payment Card Industry Data Security Standards (PCI DSS)
- Control Objectives for Information and Related Technology (COBIT) Framework
- Center for Internet Security (CIS) benchmarks

CHAPTER 5
REPORTING

The audit report is prepared after the audit's completion and after the consolidation of all observations and/or findings. An exit meeting should be conducted to discuss the observations and finalize the contents of the draft report with management before finalization of the report.

1. **Table of Contents**: It provides easy navigation of the audit report with a list of all sections and subsections.
2. **Introduction**: It provides an understanding of the business and its environment, including key risks and opportunities.
3. **Audit Objective**: It provides the purpose of the audit and what the IS auditors expected to achieve.
4. **Audit Scope**: It helps identify the specific items included in the audit and any exclusions.
5. **Audit Methodology**: It provides an understanding of the approach and procedures used by the IS auditors to conduct the audit.
6. **Criteria for Evaluation of Controls**: It helps to understand the basis on which the IS auditors assigned severity levels to each finding. The basis on which severity levels are assigned to each finding is stated in Chapter 9.
7. **Executive Summary**: It provides a high-level overview of the audit results, including key findings, recommendations, and management's response.
8. **Detailed Findings and Recommendations**: It provides a review of each audit finding in detail, including the condition, severity level, criteria, impact, recommendation, and management response, and includes the following details:
    - Condition: observation or finding noted during the review of the item
    - Severity level of risk
    - Criteria: reference to policy, procedure, laws, regulations, standards, framework, or best practices to which observation is related
    - Impact: consequences of the observation on the enterprise
    - Recommendation
    - Management Response: Management action plans
    - Follow-up of prior period audit resolutions

    Example: Business Continuity Management

Data Backup	Medium
Condition	*On review of the status of the backup of data for the organization during our audit, we have noted the following observations:* • *The backup of the core database was maintained without encryption or password protection, and* • *The configuration backup of network devices (such as routers and switches) was maintained without encryption or password protection.*
Criteria	*As per <reference to framework/guideline/best practice>, the organization should have a data security policy and procedure in place to ensure the security of data stored or transmitted electronically. This should cover, among other things, appropriate data disposal procedures, storage of data in portable devices, security of media while in transit or storage, physical and environmental control of storage media, and encryption of customers' critical information being transmitted, transported, or delivered to other locations.*
Impact	*In the absence of encryption in database backups of critical application databases, in case of loss or theft of the storage medium, a user can view data in plain text.* *If the backup is lost, stolen, or otherwise compromised, the confidentiality of the data cannot be ensured.*
Recommendation	*It is recommended to:* • *Encrypt or keep password protection on local storage used for backups.* • *Encrypt the configuration backup of network devices with a strong encryption algorithm. The encryption key should be kept securely and not shared with unauthorized personnel.*
Management Response	The device used to store the backup file is encrypted using BitLocker.

IS auditors should distribute the audit report to the respective personnel as defined in the audit charter or as per the agreement or engagement with the auditee. The audit report is confidential, so further distribution of the report is at the discretion of top management.

CHAPTER 6
AUDIT FOLLOW-UP

6.1 Tracking Action Plans

The true value of an audit is in the constructive transformation it provides to the business. Once the IS auditor has thoroughly documented the findings and observations, his or her duty goes beyond simply reporting the issues. The auditor should encourage and ask the management to develop a thorough action plan, including exact dates for control implementation and closure of issues based on the severity of the risk.

As an IS auditor, it is essential to regularly monitor these action plans to verify their closure. This duty, as specified in the audit charter or established agreements with the auditee, entails consistent monitoring, tracking of progress, and validation of remedial measures. Auditors play a crucial role in ensuring that the organization not only acknowledges the findings but also takes measures to reduce risks and improve the security and effectiveness of its information systems.

6.2 Validation of Remediation Efforts

It is the responsibility of the IS auditors to ensure that management either executes its action plans in an efficient way or chooses to accept the risk of not resolving the issue. This decision is influenced by various factors, including cost, complexity, and other strategic considerations. As per ITAF Reporting Guidelines 2402, if management chooses to accept the risk instead of taking corrective action, they must inform the board of directors or other governing authorities about this decision. It is necessary to officially record and authorize the acceptance of risk with the involvement of top management and communicate it to important stakeholders in order to ensure transparency and accountability.

When the auditors consider the auditee's accepted level of residual risk to be unsuitable, it is important to discuss this with executive management. Furthermore, if the debates continue, it is advisable to bring the matter to the attention of the board or the individuals responsible for overseeing the organization. This escalation, conducted in cooperation with top-level management, guarantees that all possible risks are comprehensively assessed and that decisions are made in the organization's utmost interest regarding security and compliance. Therefore, the IS auditors can ensure that the organization is protected against risks and build a culture of mature risk management.

6.3 Escalation Procedures

ITAF Reporting Guidelines 2402: Follow-up Activities state that a comprehensive report on the status of agreed-upon corrective actions arising from audit reports, including any outstanding recommendations, must be presented to the relevant levels of management and governance committees, such as audit.

Furthermore, during subsequent audits, if the IS auditor discovers that corrective actions reported as "implemented" have not been executed, they should promptly communicate this status to the appropriate levels of management and governance. If necessary, the auditor should obtain an updated corrective action plan along with planned implementation dates.

CHAPTER 7
AUDIT TOOLS & TECHNOLOGY

7.1 Computer Assisted Audit Techniques/Tools (CAATs)

Computer-Assisted Audit Techniques and Tools (CAATs) are essential for IS auditors to efficiently gather and analyze data from a variety of hardware and software environments, data structures, and record formats during an audit. These tools are invaluable in both the planning and execution phases of an audit, enhancing the accuracy and thoroughness of the process.

Different types of CAATs include:

- Generalized Audit Software: This category encompasses generalized audit software (GAS), customized programs, and utility software. These tools can read various records and files, perform indexing, sorting, merging with other files, filtering, and execute statistical functions such as sampling and frequency analysis, along with various arithmetic operations. In the case of an IS audit, GAS tools can be used to identify suspicious patterns such as an abrupt increase in failed login attempts, off-hour activities, etc.
- Test Data and Scripts: Auditors use test data to identify logical errors in programs and verify that programs meet their specified requirements. This testing can occur in separate processing environments, live environments, or by embedding test code directly into the program. It involves creating specific data sets or scripts to test the functionality and controls of systems and applications. In the case of IS audits, tools such as vulnerability assessment and network analysis fall into this category.
- Audit Automation and Expert Systems: These systems are query-based and built on the extensive knowledge base of experienced auditors. They serve as a valuable resource pool during the audit, providing insights and guidance based on previous audits and expert knowledge. Furthermore, these tools can be used to automate the overall audit process through continuous monitoring. Some of the popular tools in this category are AuditBoard, Vanta, etc.

  When employing CAATs, the IS auditors must consider several factors to ensure their effective use. These include obtaining permission from the auditee to use these tools within their system, ensuring compatibility with the existing systems, and maintaining the integrity and security of the system being audited.

CAATs can be used in various aspects of an audit, such as:

- Compliance testing refers to the process of verifying that an organization's systems, controls, and processes adhere to relevant regulatory requirements and internal policies. This type of testing is critical for ensuring that the organization operates within the legal and regulatory framework and meets its own standards for governance, risk management, and compliance.
- Substantive testing involves conducting thorough examinations of specific transactions and account balances to verify their accuracy and completeness. This process is a critical component of an audit, where the auditors review the underlying documentation and record. In the case of an IS audit, substantive testing is used to evaluate the effectiveness of security controls by directly

examining the confidentiality, integrity, and availability of the underlying systems, applications, and data. For example, it can be used to test password security control by performing activities such as a review of policy, sample selection, and analysis of password strength.

IS audits can encompass both substantive testing and compliance testing, and activities such as configuration review, network and system review, source code review, vulnerability assessment, and penetration testing can contribute to both aspects.

- Configuration Review: It involves examining the configuration settings of IT systems to ensure they align with best practices, organizational requirements, and regulatory standards. From a substantive testing perspective, configuration review aims to verify the accuracy, completeness, and reliability of system configurations, ensuring they support the organization's operational needs securely. On the other hand, from a compliance standpoint, configuration review ensures that systems adhere to relevant regulations and standards, such as those concerning data protection, access controls, and security configurations. By assessing configurations, organizations can not only enhance the security posture of their systems but also ensure compliance with regulatory requirements.
- Vulnerability Assessment: It is a process of systematically identifying, evaluating, and addressing security weaknesses within an organization's IT systems. This involves scanning networks, applications, and devices to detect potential vulnerabilities that could be exploited by cyber threats. Using both automated tools and manual techniques, the assessment uncovers issues such as outdated software, misconfigurations, weak passwords, and missing patches. Identified vulnerabilities are then analyzed to determine their potential impact and associated risk levels. The primary objective of a vulnerability assessment is to gain a comprehensive understanding of the organization's security posture, prioritize vulnerabilities based on their severity, and recommend appropriate remediation actions to enhance overall cybersecurity defenses. Assessing IT systems for vulnerabilities serves as both compliance and substantive testing. Substantively, vulnerability assessment helps identify weaknesses and potential risks within IT infrastructure, applications, and networks, ensuring their integrity and resilience against cyber threats. From a compliance perspective, it ensures that systems adhere to regulatory requirements related to data protection, cybersecurity, and risk management. By conducting vulnerability assessments, organizations can mitigate security risks while also demonstrating compliance with applicable laws, regulations, and industry standards.
- Network and System Review: It is a comprehensive assessment of network architecture and system designs that serves both substantive and compliance testing purposes. Substantively, this review evaluates the overall integrity, reliability, and effectiveness of IT infrastructure, identifying weaknesses and potential points of failure. Simultaneously, from a compliance perspective, it ensures that network and system configurations align with regulatory mandates and industry standards. By examining network and system designs, organizations can address security vulnerabilities while also demonstrating adherence to legal and regulatory requirements.
- Source Code Review: It is used to review the source code of software applications and serves dual purposes in both compliance and substantive testing. Substantively, source code review aims to identify security vulnerabilities, coding errors, and potential risks that could compromise the integrity and functionality of the software. From a compliance standpoint, it ensures that software

development practices comply with relevant regulations, industry standards, and organizational policies. By reviewing source code, organizations can strengthen the security of their software assets while also demonstrating compliance with legal and regulatory requirements.

- Penetration Testing: It simulates real-world cyberattacks through penetration testing, which offers benefits for both compliance and substantive testing purposes. Substantively, penetration testing evaluates the effectiveness of security controls and defenses, identifying weaknesses and vulnerabilities that could be exploited by malicious actors. From a compliance standpoint, it ensures that organizations meet regulatory requirements for safeguarding sensitive information and protecting against cyber threats. By conducting penetration tests, organizations can strengthen their security posture while also demonstrating compliance with legal, regulatory, and industry standards.
- Others: Activities such as incident investigation, threat hunting, and forensic analysis are critical for testing the effectiveness of security controls. These activities help identify detection and alerting capabilities, verify data integrity, analyze malware, and respond to incidents.

7.2 Data Analytics in Auditing

Data analytics is vital in IS auditing as it enables the auditors to efficiently analyze large volumes of data to identify anomalies, patterns, and trends that may indicate potential risks or irregularities. For instance, the auditors can use data analytics tools to analyze transactional data and system logs to detect fraudulent activities, such as unauthorized access or suspicious transactions. Additionally, data analytics can help the auditors monitor compliance with regulatory requirements by analyzing data to ensure adherence to established controls and procedures, such as GDPR compliance through analyzing data access patterns or PCI-DSS compliance by examining payment transactions. Moreover, data analytics enhances audit effectiveness by allowing the auditors to automate repetitive tasks and perform more comprehensive audits, thus providing valuable insights to stakeholders and supporting informed decision-making within organizations. Below are some examples where data analytics is required in an IS audit:

- IS auditors can use data analytics tools to extract users' roles and permissions from organizational systems and analyze transaction logs to track user activities. By comparing this data, the auditors can identify instances where users have access to transactions beyond their designated roles, highlighting potential segregation of duties violations. This analysis allows the auditors to evaluate the effectiveness of segregation of duties controls, identify non-compliance, and recommend corrective measures to mitigate associated risks, thereby enhancing the overall integrity and security of the organization's transactional processes.
- Classification algorithms, such as logistic regression and support vector machines, play a crucial role in detecting fraud and abnormalities within organizational data. These algorithms can identify fraudulent or anomalous patterns. For instance, logistic regression can model the probability of a transaction being fraudulent based on various features, while support vector machines (SVM) can identify complex patterns in high-dimensional data to distinguish between normal and anomalous behavior. By leveraging these algorithms, IS auditors can automate the process of fraud detection, efficiently identifying suspicious transactions or activities that require further investigation. This enhances the effectiveness of fraud detection efforts and enables the

auditors to proactively mitigate risks associated with fraudulent behavior, thereby safeguarding the organization's assets and reputation. Similarly, clustering algorithms can be used to identify outliers or abnormal patterns in clusters.

- A review of logs can be used to identify suspicious activities such as multiple failed login attempts, unusual connections, file access attempts, etc. These are particularly important for detecting potential breaches. By analyzing system logs, IS auditors can identify patterns of failed login attempts, which may indicate unauthorized access attempts or malicious activity. For example, a sudden spike in failed login attempts from unusual locations or at odd hours could signal a security threat. Additionally, file monitoring involves examining access logs and changes made to sensitive files or directories, enabling the auditors to track user actions and detect any unauthorized modifications or data breaches. These practices rely on thorough analysis of log data to identify anomalies and security incidents, allowing the auditors to take prompt corrective actions and strengthen the organization's security posture.
- Testing of system conversion involves verifying the accuracy, completeness, and reliability of data and processes during the migration or conversion of systems, such as transitioning to a new software platform or upgrading existing systems. Data analytics approaches can be employed in this testing process to enhance the effectiveness and efficiency of IS audits. For instance, IS auditors can utilize data analytics tools to analyze large datasets generated during system conversion to identify discrepancies, inconsistencies, or errors in the migrated data. By comparing data before and after conversion, the auditors can detect anomalies, validate data integrity, and ensure the successful transfer of critical information. Furthermore, data analytics techniques such as trend analysis and outlier detection can help the auditors identify potential issues or patterns that may require further investigation.
- By using data analytics techniques, IS auditors can analyze the access logs and compare them with employees' roles and permissions. With this, the auditors can verify whether the users accessing the system are authorized employees or not. Discrepancies between the two records, such as unauthorized users accessing sensitive data or employees with excessive access privileges, can be flagged for further investigation. This data analytics approach enhances audit efficiency by automating the process of identifying access control weaknesses or violations, ultimately helping organizations strengthen their security posture and mitigate risks associated with unauthorized access or data breaches.
- Matching inbound data with outbound data to identify tailgating is a data analytics approach used in physical security auditing to enhance the monitoring and detection of unauthorized access incidents. IS auditors can analyze records of entry and exit activities captured by physical security systems, such as access control systems or surveillance cameras. By comparing the timestamps and identity records, the auditors can detect suspicious activities. Any instances where multiple users enter using a single access credential or where an individual exits without a corresponding entry record can be flagged as a potential tailgating event.

7.3 Remote Auditing Technologies

As remote working becomes increasingly popular, so does the practice of remote audit execution. However, it is important to understand the complexities of remote engagements and for both parties to agree on the approach and the planning process. A successful remote audit utilizes technologies such

as video conferencing (e.g., Zoom), screen-sharing software (e.g., TeamViewer), document-sharing platforms (e.g., Google Drive), secure communication channels (e.g., VPNs), audit automation and expert systems (e.g., Workiva), and test data and scripts (e.g., Burp Suite). It is important to note that most testing performed on a given system or application does not allow physical access. Therefore, the IS auditor should be able to access the systems via the network, though not necessarily from outside the client's environment.

The auditor should discuss and agree on who is responsible for the facilitation of such solutions from both sides. Both parties should agree on the types of documents and information that can be accessed, viewed, or shared based on the security, privacy, and confidentiality requirements.

CHAPTER 8
AUDIT QUALITY ASSURANCE

8.1 Quality Control Framework

In accordance with ITAF Performance Standard 1204: Performance and Supervision, the audit should involve the supervision of IT audit staff to ensure the achievement of audit objectives and adherence to professional audit standards. Therefore, it is essential for the IS auditors to establish a robust quality control framework or process. This framework should facilitate objective evaluations to ascertain the appropriateness of significant judgments made by the audit team and the conclusions reached in formulating the audit report.

For guidance in developing a quality control framework, IS auditors should refer to the Nepal Standard on Quality Control (NSQC 1), which provides quality control for firms performing audits and reviews of financial statements and other assurance and related service engagements, issued by the Auditing Standard Board of Nepal. This standard outlines principles and procedures for implementing effective quality control measures within audit practices, ensuring the delivery of high-quality audit services to clients.

8.2 Quality Control Review

The audit should include a quality control review of the IS audit engagement to ensure the accuracy, reliability, and completeness of the audit process and deliverables. This review may be conducted by either an experienced internal team within the auditing firm or by an external professional with relevant expertise. Importantly, the reviewer should not be a part of the audit team to maintain objectivity and independence in the review process. During the quality control review, the reviewer should evaluate various aspects of the audit engagement, including:

8.2.1 Adherence to audit standards and guidelines

Adherence to audit standards and guidelines is very important for effective auditing. During a quality control review, IS auditors ensure that their practices align with established industry standards, regulatory requirements, and internal guidelines. This adherence ensures that audits are conducted with integrity and credibility, upholding recognized best practices and benchmarks. By following these standards, the auditors provide stakeholders with confidence that the audit process meets rigorous standards and delivers reliable results.

8.2.2 Compliance with established audit methodologies and procedures

Compliance with established audit methodologies and procedures is paramount to maintaining consistency and reliability in audit outcomes. IS auditors must adhere to predefined audit methodologies and procedures consistently throughout the audit process. This ensures that audits are conducted in a systematic and structured manner, enabling the auditors to obtain reliable evidence and draw accurate conclusions. Compliance with these methodologies enhances the reliability and consistency of audit results, fostering stakeholder trust in the audit process.

8.2.3 Accuracy and completeness of audit documentation

The accuracy and completeness of audit documentation are critical components of a quality control review. IS auditors should document their findings, evidence, and conclusions in detail to provide a comprehensive record of the audit process and outcomes. Complete and accurate documentation ensures transparency and accountability, allowing stakeholders to understand the basis of audit conclusions and recommendations. Thorough documentation also facilitates effective communication and decision-making, enabling stakeholders to act on audit findings confidently.

8.2.4 Appropriateness of audit conclusions and recommendations

The appropriateness of audit conclusions and recommendations is a key focus area during a quality control review. IS auditors must ensure that their conclusions are logically derived from the evidence collected and analysis conducted during the audit process. Additionally, audit recommendations should be practical, feasible, and tailored to address identified risks and deficiencies effectively.

8.2.5 Effectiveness of communication with stakeholders

Effective communication with stakeholders is essential for the success of an audit. IS auditors must communicate clearly, transparently, and timely with stakeholders throughout the audit process. Clear communication fosters trust, collaboration, and understanding, ensuring that stakeholders are informed and engaged in the audit process. By keeping stakeholders informed of audit progress, findings, and recommendations, the auditors facilitate informed decision-making and promote accountability and ownership of audit outcomes.

8.2.6 Overall quality and consistency of the audit report

Finally, the overall quality and consistency of the audit report are paramount. The audit report serves as the primary deliverable that communicates audit findings, conclusions, and recommendations to stakeholders. Reviewers assess the structure, organization, and presentation of the audit report to ensure clarity, coherence, and comprehensiveness. Additionally, they evaluate the report's objectivity, balance, and supportiveness of the audit findings with sufficient evidence and analysis. A well-crafted audit report provides stakeholders with a clear understanding of the audit process, outcomes, and implications, enabling them to make informed decisions and take appropriate actions.

CHAPTER 9

ANNEXURE

9.1 Audit Checklist

9.1.1 IT Governance

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Whether the structure of the organization is appropriate for its nature and size?			
2.	Whether roles and responsibilities are defined as per structure and are appropriate?			
3.	Are the Boards and Directors in the organizations involved in IT, information security and privacy governance through different committees? *[Obtain list of committees, terms of reference of the committees and their members.* *Obtain minutes of IT Strategy and Steering Committee, if any.]*			
4.	Whether the business strategy and objective are formulated and aligned with IT? *[Verify the document is approved by the management.]*			
5.	Whether the Policy formulated by the organization is endorsed, relevant, realistic, attainable, adaptable, enforceable, and Inclusive?			
6.	Whether Policies support and agree with relevant laws, regulatory guidelines, directives, circulars, international frameworks and standards and contractual obligations?			
7.	Whether standards, guidelines, plans, and procedures are developed to support the implementation of policy objectives and requirements?			
8.	Whether the policies are communicated to all relevant parties both within and external to the organization? *[Obtain the evidence of communication such as email, internal circulars, etc.]*			
9.	Whether policies reviewed at planned intervals to ensure their continuing suitability, adequacy, and effectiveness?			

9.1.2 Information Security Risk Management

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Information Security Risk Management			
1.	Is information security risk considered as a part of enterprise risk management? *[Review the risk management policy of the enterprise]*			
2.	Whether the organization has specific IT risk management policy/procedures?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
3.	Ensure the IT Risk Management policy/procedures provisions at least the following: - Risk governance structure - Roles and responsibilities for risk management - Risk identification, assessment, and evaluation procedures - Risk response - Responsibilities for risk identification - Risk register			
4.	Verify and IT risk appetite and tolerance level of the organization.			
5.	Whether the risk assessment is performed by the organization and risk register has been maintained and updated? [*Obtain and evaluate the evidence of the Risk assessment report and Risk register]*			

9.1.3 Compliance

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Compliance with Legal Requirements			
1.	Are all information system security related statutory, legal, regulatory and contractual understood and documented?			
2.	Is there a process to stay informed about changes in the requirements?			
3.	Are there controls to ensure compliance with the requirements?			
4.	Are there regular audits and reviews to ensure compliance?			
5.	Is there a process in place for addressing non-compliance and making necessary improvements?			
6.	Are there procedures for preserving organizational records in compliance with requirements?			
7.	Are there processes for ensuring the protection of records, including privacy and intellectual property rights?			
8.	Are there procedures to comply with the secure disposal requirements defined by laws, regulations, and contracts?			
	Compliance with Security Policies and Standards			
9.	Are regular reviews and audits conducted to ensure compliance with applicable standards and organizational security policies?			
10.	Are deviations from security standards and policies recorded and addressed?			
11.	Is there a process in place for updating and improving security policies and standards based on audit findings?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
12.	Are all employees and third parties aware of the security policies and their obligation to comply with them?			
13.	Is there a process in place for addressing non-compliance by employees, contractors, and third-party users?			
14.	Are there guidelines in place to ensure the secure design and development of in-house developed systems?			
15.	Are information systems regularly checked for compliance with security policies and standards?			
16.	Are the security implications of changing the business processes considered and addressed?			
	Technical Compliance Checking			
17.	Are regular technical compliance checks performed?			
18.	Are there regular checks to ensure the use of correctly licensed software?			
19.	Are information systems checked for compliance with security implementation standards?			
20.	Are there regular vulnerability assessments or penetration tests of systems and networks?			
21.	Is there a process in place for addressing non-compliance and vulnerabilities found during technical compliance checks?			
22.	Are there checks on systems to ensure that software patches are up to date?			
23.	Are there checks on systems to detect the presence of unauthorized software?			

9.1.4 Asset Management

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Assets Management			
1.	Whether the organization has asset management policy that has provisions for acquisition, maintenance, and disposal of IT assets?			
2.	Whether there is appropriate procedure for moving assets from one place to another? *[Evaluate procedure and examine such instances, if any.]*			
3.	Whether the organization has information classification guidelines?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
4.	Ensure the organization has inventory record of information asset with at least following information for each of the assets and verify the information on sample basis: - A clear and specific identification of the asset - Its location - Its security/risk classification - Its group - Its owner - Its designated custodian			
5.	Whether owners must authorize internal information and information system access rights and permissions? *[Access rights and permissions must be reviewed and approved periodically.]* *[Obtain the evidence of authorization provided.]*			
6.	Whether a process in place for asset owners to periodically review owned assets to ensure the accuracy of asset information (e.g., classification)?			
7.	Is there a practice of physical verification of IT assets?			
8.	Whether procedures in place outlining appropriate destruction of electronic media, including procedures for removing sensitive data prior to re-use or disposal?			

9.1.5 Human Resources Security

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Prior to Employment			
1.	Whether the roles and responsibilities for information security included in job descriptions?			
2.	Do employment contracts/agreements include appropriate terms for information security?			
3.	Is background verification carried out as part of the recruitment process, based on the risk of the job role?			
4.	Are all employees given a copy of the information security policy and adequately briefed?			
5.	Are the employees provided with information security awareness training as a part of orientation/induction training?			
6.	Is there a process (tests, quizzes) to verify the effectiveness of information security awareness training?			
7.	Are non-disclosure agreements used where appropriate?			
	During Employment			
8.	Are there programs in place periodically to raise and maintain employee awareness about information security?			
9.	Are there procedures to monitor and respond to breaches of information security by employees?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
10.	Is information security included in the performance review?			
11.	Is there a disciplinary action defined for violation of information security policies?			
	Termination			
12.	Is there a formal process for the return of organizational assets upon termination of employment?			
13.	Are exit interviews conducted to remind leaving employees of their ongoing responsibilities for information security?			
14.	Is there a procedure to monitor suspicious activities related to an employee's impending departure?			
15.	Are there measures in place (fallback staff or any other measures) to ensure the continuity of necessary operations after an employee's departure?			

9.1.6 Operations Security

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Are access controls implemented effectively to ensure that only authorized personnel have access to systems			
2.	Is there an established incident response plan in place			
3.	Are monitoring and logging mechanisms in place to track user activities			
4.	Is there a structured patch management process to regularly update software			
5.	Is there a comprehensive security awareness training program for employees to educate them about security threats			
6.	Other questions as applicable to specific domain			

9.1.7 Endpoint Security

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Whether the endpoint security policy or procedures is formulated?			
2.	Is awareness training provided to staff regarding the risks associated with malware?			
3.	Whether the antivirus and antimalware installed on the server and end-user device?			
4.	Whether signatures of anti-malware/ endpoint security software get updated automatically from the internet and updates are pushed to other servers, and workstations regularly? *[Verify the settings cannot be changed from workstations.]*			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
5.	Whether windows security patches updated on individual workstations?			
6.	Whether admin access disabled on user workstations?			
7.	Whether external Removable media (CD/DVD, Pen drives) is disabled on workstations without exceptional approvals?			
8.	Is installation of unauthorized software restricted?			
9.	Whether usage of social media and personal e-mail restricted (unless there is approval for use for business purpose)?			
10.	Ensure hardening policies are effectively enforced in workstations and servers. *[Full Disk Encryption, Screen timeout, Password policy, etc. can be reviewed.]*			

9.1.8 Physical & Environmental Security

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Secure Areas			
1.	Are there designated secure areas to protect critical or sensitive information assets?			
2.	Are there controls in place to prevent unauthorized access to secure areas?			
3.	Are access rights to secure areas regularly reviewed and updated?			
4.	Are there measures to protect secure areas from physical threats such as fire, flood, etc.?			
5.	Are there procedures in place for visitors, including sign-in, escorts, and badge requirements?			
6.	Is there CCTV or other surveillance equipment to monitor secure areas?			
7.	Are there measures in place to prevent eavesdropping or unauthorized information gathering in secure areas?			
8.	Is there a process to assess the physical security measures of third-party vendors with access to sensitive information?			
	Equipment Security			
9.	Are there policies in place for using and maintaining organizational equipment securely?			
10.	Are there procedures to prevent theft, damage, and unauthorized access to organizational equipment?			
11.	Are there rules in place for removing equipment from the organization's premises?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
12.	Are there controls to protect equipment and power cables from physical and environmental threats?			
13.	Is there a secure disposal or reuse process for equipment?			
14.	Is there a process for managing equipment maintained by third parties?			
15.	Is there a system in place to maintain up-to-date inventory of all equipment?			
16.	Are all types of equipment (e.g., IT equipment, security equipment, etc.) covered under the equipment security policy?			

9.1.9 Business Continuity Management

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Business Continuity Plan Policy and Procedures			
1.	Is there a business continuity and disaster recovery plan that addresses the loss of information or processing capabilities?			
2.	Whether the policy, procedures, or plan includes the following elements: - Condition for activation of plan - Roles and responsibilities - Call Tree - Relocation Strategies - Operational Management - Communication - Recovery Strategies - Testing of plan			
3.	Is the business continuity plan regularly tested and updated?			
4.	Are the organization's critical business processes identified and Business Impact Analysis conducted before formulating business continuity plan?			
5.	Whether the disaster recovery plan includes recovery strategies and procedures for systems and facilities as determined by the business impact assessment?			
6.	Does the plan consider information security requirements in the event of disaster?			
7.	Are there backups and redundancy strategies?			
8.	Are there measures to deal with the loss of third-party services or suppliers?			
9.	Is there a training and awareness program in place for business continuity plans?			
10.	Is there a clear understanding of which staff roles and responsibilities are crucial in the case of a disaster?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Redundancy			
11.	Whether there are redundancy strategies in place to ensure availability of information and assets?			
12.	Are these strategies regularly tested and updated?			
13.	Are there fail-over mechanisms in place to ensure service continuity in case of a system failure?			
14.	Are there plans in place to deal with the loss of third-party services or suppliers?			
15.	Are all redundancy systems protected and secured at the same level as the primary systems?			

9.1.10 Incident Management

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Policy and Procedures			
1.	Whether the Policy and procedures related to Incident Response are formulated?			
2.	Whether an organization defines criteria for an event to an information security incident?			
3.	Whether the incident severity level matrix is formulated by the organization?			
4.	Whether incidents classified by severity relative to the impact they have on an organization? [*The level of incident can be classified as below:* *Level 1: Incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation.* *Level 2: Incidents are defined as a compromise of or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation.* *Level 3: Incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel. There is no evidence or suspicion of harm to customers or proprietary information, processes, or services.]*			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
5.	Whether an incident response plan is maintained to ensure that information security incidents are responded to, managed, and reported consistently and effectively? [*The incident response plan may include the following:* - *Preparation* - *Detection and investigation* - *Initial response* - *Containment* - *Eradication and recovery* - *Notification* - *Closure and post-incident activity* - *Documentation and evidence handling]*			
6.	Whether all employees, contractors, consultants, and vendors received incident response training appropriate to their role?			
7.	Whether an incident response team (IR Team) is established? [*Verify the establishment of an incident response team involves the following steps not limited to:* - *Defining the incident response team constituency.* - *Ensuring management and executive support.* - *Ensuring budget allocation.* - *Deciding where the IR Team will reside within the organization's hierarchy.* - *Determining whether the team will be central, distributed, or virtual.* - *Developing the process and policies for the team.]*			
	Reporting Information Security Incidents			
8.	Is there a formal event reporting and escalation process?			
9.	Are users (including managers) aware of information security reporting responsibility?			
10.	Are there mechanisms for reporting security incidents to external parties where relevant (e.g., cybercrime reporting to NRB by BFIs)?			
11.	Are employees trained on incidents recognition and reporting?			
12.	Is there a process for reporting the loss or compromise of information assets?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
13.	Are there measures in place to minimize damage from incidents and to restore systems to normal operation as quickly as possible?			
	Management of Information Security Incidents			
14.	Is there a process for responding to and managing information security incidents?			
15.	Is there a process for implementing necessary improvements to organizational policies and procedures following an incident?			
16.	Is there an incident response team that is adequately resourced and trained?			
17.	Are incidents classified based on severity and business impact?			
18.	Are lessons learnt from past incidents reviewed and used to improve the incident management process?			
19.	Is there a review process of a past incident to assess the effectiveness of the response?			
20.	Are the results of incident reviews used to improve the organization's security posture?			
21.	Are there procedures for evidence collection and forensics?			

9.1.11 System Acquisition, Development and Maintenance

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Security Requirements of Information Systems			
1.	Is there an information security requirements analysis and specification process in place for all systems?			
2.	Is there a process for ensuring that all information processing systems meet the information security requirements?			
3.	Is there a process for defining and implementing controls to ensure the accuracy and completeness of information outputs?			
4.	Are there checks to ensure that the security requirements of installed systems are being fulfilled?			
5.	Is there a regular review of the organization's business processes, information flows, and systems?			
6.	Are there processes to identify and assess system risks?			
7.	Is there a process to ensure that the systems' security requirements are updated to reflect changes in the business and external environment?			
8.	Are there procedures in place for the secure development and testing of systems?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Correct Processing in Applications			
9.	Are there procedures in place for detecting and correcting errors in processing?			
10.	Are there procedures in place for ensuring data integrity during processing?			
11.	Are there controls in place to prevent or detect the unauthorized manipulation of software?			
12.	Is there a process for ensuring that transaction errors are detected and handled appropriately?			
13.	Are there checks to verify processing completeness and accuracy?			
14.	Are there measures in place to guarantee the authenticity and integrity of inputs, outputs, and processing?			
	Cryptographic Controls			
15.	Are cryptographic controls regularly reviewed and updated?			
16.	Is encryption used for transmitting sensitive data over public networks?			
17.	Are there procedures in place for the use of digital signatures?			
18.	Is the integrity of sensitive or critical information ensured using cryptographic techniques?			
19.	Are there controls in place to protect sensitive data in storage using cryptographic techniques?			
	Security of System Files			
20.	Are there controls to secure system files?			
21.	Is there access control to protect system files?			
22.	Are there controls to ensure the integrity of system files?			
23.	Is there a process for the secure development and testing of system files?			
24.	Is there a process to restrict the application installation on operating systems?			
25.	Are there controls in place to manage system changes and upgrades?			
	Security in Development and Support Process			
26.	Are there secure development policies in place?			
27.	Is there a formal change control process?			
28.	Are there technical reviews of applications after operating system changes?			
29.	Are there controls to prevent changes on software packages?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
30.	Are there controls on information leakage from system development environments to operational environments?			
31.	Are there controls to ensure the separation of duties between developers and operational staff?			
32.	Is there a secure system engineering process in place?			
33.	Is there a formal process in place for system acceptance?			
	Technical Vulnerability Management			
34.	Is there a process for collection of information regarding technical vulnerabilities in time?			
35.	Is the organization's exposure to such vulnerabilities evaluated?			
36.	Is there a process for timely remediation of the identified vulnerabilities?			
37.	Are there controls to prevent exploitation of technical vulnerabilities?			
38.	Are vulnerabilities regularly checked through penetration testing or vulnerability assessments?			
39.	Are patches for vulnerabilities applied in a timely manner?			
40.	Is there a process for ensuring security of outsourced software development?			
41.	Are there controls to identify and protect against malicious code in software's?			

9.1.12 Third Party Service Assessment

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Are there controls and procedures for identifying and managing risks associated with third-party services?			
2.	Are third-party services defined and regulated through contracts or agreements?			
3.	Is there defined and agreed upon service level agreement and non-disclosure agreement?			
4.	Are there procedures for monitoring and reviewing third-party services?			
5.	Are third-party access rights reviewed and updated regularly?			
6.	Is there a process for handling breaches of contract by third-party service providers?			
7.	Is there a procedure to ensure the secure disposal or return of assets at the termination of a contract?			
8.	Are there contingency plans in case the third-party provider fails to deliver?			

9.1.13 Access Control

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	General			
1.	Is there a defined process for granting and revoking access rights for new employees?			
2.	Are changes in a role or responsibility accompanied by a review and adjustment of access rights?			
3.	Are there procedures for revoking access rights when an employee leaves the organization or changes job roles?			
	Network Access Control			
4.	Are there policies and procedures for protecting information systems from unauthorized network access?			
5.	Is there a secure log-on process for networks and network services?			
6.	Are there measures in place to manage the connection of mobile devices to the office network?			
7.	Is the principle of least privilege used for providing network access?			
8.	Are there controls in place to prevent network traffic from systems that do not need to connect to the network?			
9.	Is the use of active network services (such as email, internet, and databases) controlled and properly protected?			
10.	Are network segregation controls in place?			
11.	Are network users authenticated?			
	Operating System Access Control			
12.	Are there procedures in place to prevent unauthorized access to operating systems?			
13.	Is secure login process implemented for accessing operating systems?			
14.	Are all operating system access rights reviewed and updated regularly?			
15.	Is the use of system utilities controlled?			
16.	Are session time-out controls implemented?			
17.	Are there restrictions on the connection of mobile devices and external storage devices?			
18.	Are password management systems interactive and ensure quality passwords?			
19.	Are all activities performed by privileged roles logged and monitored?			
	Application Access Control			
20.	Are there procedures in place to prevent unauthorized access to applications?			
21.	Is secure login process implemented for accessing applications?			
22.	Are all application access rights reviewed and updated regularly?			
23.	Are session time-out controls implemented for applications?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
24.	Is there a policy against the use of application system utilities that might be capable of overriding system and application controls?			
25.	Are restrictions in place on information input via applications?			
26.	Is logging and monitored performed privileged roles in the applications.			
	Monitoring System Access and Use			
27.	Is there a process for logging and monitoring system access and user activities?			
28.	Are all logged events reviewed regularly?			
29.	Are system logs protected against tampering and unauthorized access?			
30.	Are the clocks of all relevant information processing systems synchronized?			
31.	Are there measures to collect and store evidence to support event analysis and legal action?			
32.	Are event logging and the protection of log information minimally compliant with legal requirements?			
33.	Are procedures in place to link all access to systems and procedures with individual users?			
34.	Is there a process to respond to anomalies in timely manner?			

9.1.14 Network and Communication Security

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Network Security			
1.	Whether the policies and procedures formulated for network security?			
2.	Whether the Network Devices (Firewall, Switch, Router) in High Availability?			
3.	Whether Centralized Network Devices and Network Monitoring are in use?			
4.	Whether resource monitoring tools are used for monitoring the performance, CPU usage storage, etc..?			
5.	Whether public and private Zones for servers segregated?			
6.	Are there firewall and gateway controls in place at each network boundary?			
7.	Whether network segregated department-wise?			
8.	VLAN is segregated for all the departments?			
9.	Whether Network Devices (Firewall, Switch, Router) licensed?			
10.	Whether organization access management policy applicable to network security?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
11.	Whether configuration backup of Network devices maintained both on the external hard drive and online?			
12.	Whether backup maintained encrypted?			
13.	Whether backup configurations tested on planned intervals?			
14.	Is configuration document restoration available?			
15.	Whether provisions for Vendor access to the Network devices an organization access management policy?			
16.	Whether the single-point failure is avoided in the firewall and switch?			
17.	Whether email filtering or spam protection is maintained or not?			
18.	Is the LOG for network devices maintained?			
19.	Whether patch management is performed in planned intervals?			
20.	Whether the Network Hardening Policy formulated?			
21.	Is the network drill conducted in planned intervals?			
22.	Are vulnerability scans and penetration tests conducted regularly on the network infrastructure?			
	E-mail Security			
23.	Whether Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) has been enabled in the organization's e-email? server and are functioning as required?			
24.	Whether spam filter has been configured?			
25.	Can malicious attachments be detected? Ensure there is restriction in attachment size and file types (such as .exe, .bat, .vbs).			
26.	Ensure a strong password policy is enforced for all users.			
27.	Can email be encrypted?			
28.	Is multifactor authentication enabled?			

9.1.15 Cloud Security

S.N	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
	Cloud Security Policies			
1.	Is there a proper and up to date cloud security policy?			
2.	Do employees receive regular security training related to cloud services?			
3.	Is there an effective incident response plan?			
	Cloud Provider Compliance			
4.	Do the cloud providers have compliance certifications and audit reports?			

S.N	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
5.	Are security assessments conducted for the cloud provider's security practices?			
	Identity and Access Management (IAM)			
6.	Is MFA enforced for all privileged accounts and sensitive data access?			
7.	Is there RBAC policy to ensure users have appropriate access permissions?			
8.	Are there access logs to check for any unauthorized access attempts?			
9.	Do administrative accounts require temporary activation and are not permanently active?			
	Data Encryption			
10.	Validate that customer-controlled encryption key is used encrypt data stored in the cloud.			
11.	Check network logs to confirm that data transmissions are encrypted			
12.	Review the backup configurations to ensure data backups are encrypted			
13.	**Cloud API Security:** Review API access controls and validate the implementation of authentication mechanisms			
14.	**Secure API Integration:** Evaluate the security practices in place for API integration			
15.	**Asset Inventory:** Validate the asset inventory against cloud service usage and configuration.			
16.	**Secure Data Deletion:** Verify that data is securely deleted and not recoverable after deletion			
17.	**Cloud Compliance Monitoring:** Review compliance monitoring reports and validate compliance with security policies			
18.	**Encryption Key Management:** Review and validate key management rotation practices. Verify that encryption keys are regularly rotated as per the defined key management policy			
	Cloud Access Reviews: Validate that access reviews are conducted at appropriate intervals			
19.	**Cross-Account Access Control:** Verify that cross-account access is appropriately managed and restricted			
20.	**Secure Data Transfer to the Cloud:** Confirm that data transfer protocols use secure encryption methods.			
21.	**Geolocation Restrictions**: Validate that data is stored and processed only in approved locations			
22.	**Data Privacy and Compliance:** Review data privacy policies and processes for compliance			

S.N	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
23.	**Secure Cloud Deployment Models:** Review the organization's cloud deployment models (public, private, hybrid, community) and validate if they are appropriate			
24.	**Cloud Incident Management:** Review the cloud specific incident management plan and evaluate its effectiveness			
25.	**Cloud Provider Incident Response:** Review the cloud provider's incident response plan and assess its effectiveness			
26.	**Secure Cloud Storage:** Review cloud storage configurations against security best practices			
27.	**Secure Cloud File Sharing:** Verify that file sharing services are securely configured, and access is restricted			
28.	**Cloud Resource Monitoring:** Ensure there is a process for monitoring resources in cloud and appropriate actions are taken, if required.			
29.	**Secure Cloud Containerization:** Validate that containers are securely configured and patched			
30.	**Secure Cloud Orchestration:** Review cloud orchestration processes and validate their security			
31.	**Secure Cloud Change Management:** Review cloud change management processes and verify adherence to procedures.			
32.	**Secure Cloud Load Balancing:** Validate that load balancers are configured securely.			
33.	**Secure Cloud Database Management:** Verify that cloud databases are securely configured, and access is controlled.			
34.	**Secure Cloud DNS Management:** Is cloud DNS configured securely to prevent DNS-based attacks?			
35.	**Cloud Security Metrics and Reporting:** Are cloud security metrics defined?			

9.1.16 Mobile Device Management

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Whether the organization has Bring Your Own Device (BYOD) policy or any other policy as appropriate to mobile device deployment model?			
2.	Is the policy on acceptable use of mobile devices documented? *[Obtain the security policy on usage of mobile devices like laptops and hand-held computing devices.]*			
3.	Are employees communicated about the use of mobile device usage policies and procedures?			
4.	Whether the organization has mobile device registration procedure?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
5.	Whether the organization has the process for identification of loss or theft of mobile devices and disabling such devices? Is this process implemented?			
6.	Whether the policy and procedure are approved by the Management?			
7.	Whether the management has analyzed the risk and business impact of using mobile devices for business purposes? *[Verify the risk and business impact analysis reports prepared by management.]*			
8.	Whether the organization has established and implemented appropriate method of the user authentication for mobile devices? *[Verify and test the user authentication methods]*			
9.	Ensure organization has approved list of applications allowed to be installed on mobile device.			
10.	Whether the organization has appropriate procedure for performing regular software updates and patches on mobile devices and has been properly implemented?			
11.	Whether the organization regularly conducts audits of mobile devices to identify and address any vulnerabilities or non-compliance?			

9.1.17 Internet of Things (IoTs) Embedded Systems

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Whether the organization has appropriate policies for governing IoT Embedded Systems?			
2.	Consider the following in reviewing IoT embedded systems:			
3.	Ecosystem Interface: - Ensure that web interface is accessible only from internal network (in case of web interface) - Ensure the interface does not allow for account enumeration, has account lockout feature, default passwords are changed, and weak credentials are not present - Ensure web interface is not susceptible to common web attacks such as XSS, SQLi or CSRF			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
4.	Authentication/Authorization: - Ensure strong passwords are required - Whether 2FA has been implemented, where possible? - Ensure password recovery mechanisms are secure - Ensure options are available for configuring password controls - Ensure credentials can be revoked - Ensure that the token/session key issuing to client is always different			
5.	Network Services: - Ensure only necessary ports are exposed and available - Ensure network ports or services are not exposed to the internet			
6.	Data Transfer: - Ensure data is encrypted using protocols such as SSL and TLS while transiting networks - Ensure only accepted encryption standards are used			
7.	Privacy Protection: - Ensure only data critical to the functionality of the device is collected and data collected is encrypted. - Ensure that any data collected is de-identified or anonymized. - Ensure that only authorized individuals have access to the personal information collected. - Ensure that end-users are provided with "Notice and Choice" if data collected is more than what would be expected from the product.			
8.	Security Configurability: - Ensure the ability to separate normal users from administrative users. - Ensure the ability to encrypt data at rest or in transit. - Ensure the ability to force strong password policies. - Ensure the ability to enable logging of security events and notify end users of security events.			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
9.	Software/Firmware: - Ensure the device can securely update. - Ensure the update file does not expose sensitive data. - Ensure the update is signed and verified before allowing the update to be uploaded and applied.			
10.	Physical Hardening: - Ensuring data storage medium cannot be easily removed. - Ensuring USB ports or other external ports cannot be used to maliciously access the device. - Ensuring device cannot be easily disassembled.			

9.1.18 Configuration & Change Management

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Whether the organization has a configuration and change management policy, process and procedures in place?			
2.	Whether the organization's Change management process includes the following at minimum: – Security patch management. – Audit trail of configuration changes. – All configuration and rule set changes of all devices and systems – Software updates and patches – System Implementation and updates – Infrastructure Change – User Access – Cloud Security and Configuration Change			
3.	Whether the inventory of configurable items has been established?			
4.	Ensure baseline system and security configurations for the items have been established and documented.			
5.	Whether the organization analyzes changes to the system to determine potential security and privacy impacts before change implementation?			

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
6.	Whether the changes required are first tested and approved?			
7.	Whether review and update the baseline configuration of the system is performed as per organization defined frequency and circumstances?			
8.	Whether request for change for each of the changes made approved?			
9.	Whether the organization has necessary procedures and processes in place for rolling back quickly when the changes to the configuration fail (fallback plan)?			

9.1.19 Cryptography

S.N.	Checklist	Yes/No/ NA	Audit Remarks	Management Remarks
1.	Whether the organization has implemented encryption mechanisms to protect sensitive data both at rest and in transit?			
2.	Whether the organization uses industry-standard cryptographic algorithms and key lengths for encryption?			
3.	Whether the organization has implemented key management practices to securely generate			
4.	Whether the organization encrypts data backups to ensure the confidentiality of sensitive information in backup storage?			
5.	Whether the organization uses digital signatures to ensure the integrity and authenticity of data and messages?			
6.	Whether the organization implements cryptographic hashing algorithms to securely hash passwords and sensitive data for storage and verification purposes?			
7.	Whether the organization has established procedures for secure key exchange and negotiation in cryptographic protocols?			
8.	Whether the organization conducts regular reviews and audits of cryptographic controls to ensure compliance with internal policies and industry best practices?			
9.	Whether the organization has documented cryptographic policies and procedures for managing cryptographic keys			
10.	Whether the organization provides training and awareness programs for employees to educate them about cryptographic best practices and procedures?			
11.	Whether the organization has established incident response procedures to handle security incidents related to cryptographic breaches or vulnerabilities?			
12.	Whether the organization has implemented cryptographic controls for secure authentication and access control mechanisms?			

S.N.	Checklist	Yes/No/ NA	Audit Remarks	Management Remarks
13.	Whether the organization performs regular vulnerability assessments and penetration testing of cryptographic implementations to identify and remediate security weaknesses?			
14.	Whether the organization has established backup and recovery procedures for cryptographic keys and materials to ensure business continuity in the event of a security incident?			
15.	Whether the organization complies with relevant cryptographic standards and regulations.			
16.	Whether the organization has implemented cryptographic controls for securing sensitive communication channels.			
17.	Whether the organization encrypts sensitive data stored on mobile devices and removable media to prevent unauthorized access in case of loss or theft?			
18.	Whether the organization has established procedures for securely disposing of cryptographic materials and decommissioning cryptographic systems at the end of their lifecycle?			

9.1.20 Monitoring & Measurement

S.N.	Checklist	Yes/No/ NA	Audit Remarks	Management Remarks
1.	Whether the company has developed a system-level continuous monitoring strategy including log and applicable data retention policy and implemented a continuous monitoring mechanism following the organization-level monitoring strategy?			
2.	Whether the organization employs independent assessors or assessment teams to monitor the controls in the system on an ongoing basis?			
3.	Whether the organization ensures risk monitoring is an integral part of the continuous monitoring strategy that includes Effectiveness monitoring; Compliance monitoring, and Change monitoring?			
4.	Whether the organization has implemented detection systems that correlate all network and system alerts with any other unusual activity across the organization?			
5.	Whether the organization has a threat intelligence and threat hunting capabilities?			
6.	Whether the organization maintains and retains logs as per organization policy or accepted standard e.g., 3 months for online storage and 3 years for offline storage.			
7.	Whether the organization has processes in place to monitor activities that are not in accordance with its security policy and may result in the loss of confidentiality, integrity and availability?			

S.N.	Checklist	Yes/No/ NA	Audit Remarks	Management Remarks
8.	Whether the organization has established key performance metrics to measure the performance of IT functions?			

9.1.21 Application Security

S.N.	Checklist	Yes/No/ NA	Audit Remarks	Management Remarks
1.	Whether the organization has implemented input controls to validate and sanitize user input to prevent injection attacks such as SQL injection or cross-site scripting (XSS)?			
2.	Whether the organization has implemented output controls to ensure that sensitive information is not disclosed unintentionally in error messages or logs?			
3.	Whether the organization has implemented processing controls to ensure that sensitive data is processed securely, such as encryption of data in transit and at rest?			
4.	Has the organization implemented integrity controls to detect unauthorized changes to data or software, such as checksums or digital signatures?			
5.	Whether the organization conducts regular vulnerability assessments and penetration testing of its applications to identify and remediate security weaknesses?			
6.	Whether the organization has implemented secure coding practices and guidelines for developers to follow during application development?			
7.	Whether the organization has established incident response procedures to handle security incidents related to application security breaches?			
8.	Whether the organization provides regular training and awareness programs for employees to educate them about application security best practices?			
9.	Whether the organization has documented policies, procedures and practice for managing access to applications and sensitive data, including user authentication and authorization mechanisms?			
10.	Whether the organization has implemented secure configuration management practices to ensure that applications are configured securely and in accordance with industry standards?			
11.	Whether the organization has established backup and recovery procedures for critical applications and data to ensure business continuity in the event of a security incident?			

S.N.	Checklist	Yes/No/ NA	Audit Remarks	Management Remarks
12.	Whether the organization conducts regular audits and reviews of its application security controls to ensure compliance with internal policies and external regulations?			
13.	Whether the organization has adopted secure development practices including secure design, threat modeling, code review, security testing, configuration management, monitoring etc?			

9.1.22 Database Security

S.N.	Checklist	Yes/No/NA	Audit Remarks	Management Remarks
1.	Has the organization implemented access controls to restrict access to the database to authorized users only?			
2.	Whether the organization has defined and enforced strong password policies for database accounts.			
3.	Whether the organization has implemented role-based access controls (RBAC) to assign permissions and privileges based on users' roles and responsibilities?			
4.	Whether the organization encrypts sensitive data stored in the database and Whether connections to database are secured using SSL/TLS?			
5.	Whether the organization conducts regular vulnerability assessments and penetration testing of the database to identify and remediate security weaknesses?			
6.	Whether the organization implements database auditing and monitoring mechanisms to track and log all database activities.			
7.	Whether the organization has established data loss prevention (DLP) policies and controls to prevent unauthorized access			
8.	Has the organization implemented database activity monitoring (DAM) solutions to detect and alert suspicious or anomalous database activities in real-time?			
9.	Whether the organization has configured secure backups of the database to ensure data integrity and availability in the event of a disaster or security incident?			
10.	Whether the organization has established procedures for secure database configuration and hardening to reduce the attack surface and mitigate common vulnerabilities?			
11.	Whether the organization has documented policies and procedures for database security management			
12.	Whether the organization conducts regular security awareness training for database administrators and users to educate them about database security best practices?			

9.2 References

1. Information Technology Audit Framework (ITAF), 4th Edition, ISACA
2. ITAF Companion Performance Guidelines 2208: Information Technology Audit Sampling, ISACA
3. Ian Cooke, “Developing the IT Audit Plan Using COBIT 2019”, ISACA Journal, 2019, Vol 3
4. CISA Review Manual (27th Edition)
5. Omar Santos. (2019). Developing Cybersecurity Programs and Policies. Pearson
6. AICPA. (2019). Audit and Accounting Manual. Wiley
7. Robert E. Davis. (2021). Auditing Information and Cyber Security Governance_ A Controls-Based Approach. CRC Press
8. *https://www.isaca.org/resources/news-and-trends/industry-news/2023/key-considerations-for-conducting-remote-it-audits*
9. *https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/advanced-data-analytics-for-it-auditors*
10. *https://www.nist.gov/cyberframework*
11. *https://cloudsecurityalliance.org/research/cloud-controls-matrix/*
12. NIST. (2018). (Cybersecurity Framework) National Institute of Standards and Technology - Framework for Improving Critical Infrastructure Cybersecurity-National Institute of Standards and Technology
13. *https://cissprep.net/domain-3-security-architecture-and-engineering/*
14. *https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project*
15. https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CCM.pdf

9.3 Abbreviations

API	Application Programming Interface
BCM	Business Continuity Management
BCP	Business Continuity Planning
BFI	Bank and Financial Institution
BYOD	Bring Your Own Device
CAAT	Computer Assisted Tools and Techniques
CCTV	Closed Circuit Television
CD/DVD	Compact Disk/ Digital Versatile Disk
CIA	Confidentiality, Integrity and Availability
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPU	Central Processing Unit
CSRF	Cross Site Request Forgery
DevOps	Development and Operations
DNS	Domain Name System
ERP	Enterprise Resource Planning
GRC	Governance, Risk and Compliance
HR	Human Resource
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICAN	Institute of Chartered Accountants of Nepal
IoT	Internet of Things
IS	Information Systems
ISA	Information System Auditor
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
ITAF	IT Audit Framework
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
NRB	Nepal Rastra Bank
NSA	Nepal Standards on Auditing
NSQC	Nepal Standards on Quality Control
NTA	Nepal Telecommunication Authority

OPSEC	Operation Security
OS	Operating System
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
RBAC	Role Based Access Control
SaaS	Software as a Service
SDLC	Software Development Lifecycle
SSDLC	Secure Software Development Lifecycle
SQLi	Structured Query Language Injection
SSL	Secure Socket Layer
SVM	Support Vector Machines
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WiFi	Wireless Fidelity
XSS	Cross Site Scripting
2FA	Two Factor Authentication

The Institute of Chartered Accountants of Nepal
ICAN Marg, Satdobato, Lalitpur, P.O. Box: 5289, Kathmandu, Nepal
Tel.: 977-1-5530832, 5530730, Fax : 977-1-5550774
E-mail: ican@ntc.net.np, Website: www.ican.org.np