सत्यमेव जयते

Comprehensive Cyber Security Audit Policy Guidelines

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Version 1.0 | 25.07.2025

Table of Contents

1. Introduction

Given the increasing number of cyber threats and the need for strong protection measures in today's digital landscape, cyber security is a major concern for enterprises. An organization's security posture can be improved, vulnerabilities detected, and regulatory compliance ensured with the help of regular cyber security audits and assessments. In an effort to promote a seamless, effective, and efficient auditing process, this document offers thorough guidance for both the auditee and auditing organizations involved in cyber security audits.

These guidelines serve two purposes. Firstly, they assist organizations being audited (auditees) in preparing for audits, understanding requirements, and addressing deficiencies. This helps ensure that their cyber security measures align with industry standards and regulations, enabling proactive improvement of security practices.

Secondly, the guidelines provide auditing organizations with a structured framework to conduct rigorous, fair, and transparent cyber security audits. They outline the auditor’s responsibilities, methodologies, and best practices, enabling them to provide independent, impartial and constructive recommendations that strengthen the auditee's cyber security.

The success of a cyber security audit relies on the collaborative efforts of both the organization being audited and the auditing entity. This document serves as a comprehensive guide to facilitate a productive partnership throughout the audit process, fostering mutual responsibility and driving meaningful enhancements in security, risk mitigation, and regulatory adherence to safeguard sensitive information.

2. Authority for Issuance of Guidelines

Whereas, sub-section (1) of section 70B of the Information Technology (IT) Act, 2000 (21 of 2000) provides that the Central Government shall appoint an agency of the Government to be called the Indian Computer Emergency Response Team and the Central Government *vide* notification dated the 27th October, 2009, has appointed the Indian Computer Emergency Response Team as the agency for the purposes of the said Act, which is now referred as CERT-In or ICERT.

And whereas, sub-section (4) of section 70B of the said Act provides that the Indian Computer Emergency Response Team shall perform prescribed functions in the area of cyber security: -

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incidents response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

And whereas, the provisions of sub-section (5) of the section 70B of IT Act, 2000 provides that the manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as prescribed and Central Government has notified Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions & duties) Rules, 2013 to this effect. The provision of rule no.9 of

these Rules, 2013, inter-alia, prescribes the activity of Information security assurance and audit to CERT-In.

And whereas, as per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person to carry out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000. The failure to provide the information or non-compliance of the direction issued under sub-section (6) attract punitive action in terms of provisions of sub-section (7) of section 70B of the IT Act.

Now, therefore, these guidelines are herein issued by CERT-In in discharge of its statutory authority and responsibility to enhance the cyber security posture of the nation, which are binding on all CERT-In empanelled auditing organizations and auditee entities covered under the relevant provisions.

3. Objective of the Document

The primary objective of this Comprehensive Cyber Security Audit Policy Guidelines document is to provide a structured and standardized framework for conducting cyber security audits within organizations. The guidelines are intended to serve as a reference for both CERT-In empaneled auditing organizations and auditee organizations to ensure that cyber security audits are carried out in a consistent, effective, and secure manner.

The document outlines the processes, methodologies, and best practices required for conducting thorough and accurate assessments of an organization's cyber security posture. It aims to:

i. Establish Uniform Standards: Ensure that all cyber security audits follow a common set of standards and procedures, thereby promoting consistency in audit quality, evaluation criteria, and reporting.
ii. Provide Clarity for Auditors and Auditees: Define the roles, responsibilities, and expectations for both auditing organizations and auditee organizations, ensuring mutual understanding of the audit process and deliverables.
iii. Promote Continuous Improvement: Encourage auditee organizations to continuously improve their cyber security measures by identifying weaknesses and implementing corrective actions, leading to enhanced overall security posture.

This document will act as a comprehensive guide for the audit process, from initial planning through to final reporting and follow-up actions, contributing to the overarching goal of safeguarding the nation's cyber infrastructure from threats.

4. Applicability

This guideline has been issued by Indian Computer Emergency Response Team (CERT-In) and is applicable to the following entities:

i. **CERT-In empaneled Auditing Organizations:** Indian Computer Emergency Response Team (CERT-In) empanels Information Security Auditing Organizations to undertake audits, including vulnerability assessments and penetration testing of computer systems, networks and applications of various organizations of the Government and of other sectors of the country. The empaneled auditing organizations agree to provide cyber security auditing services in accordance with the commercial contract to be entered into with the auditee organizations and abide by all the conditions of empanelment as well as service delivery.

ii. **Auditee Organizations:** It is the organization that owns or operates the systems, processes, and infrastructure that is being evaluated or assessed by the CERT-In empaneled auditing organisations. These guidelines are intended for organizations in both the public and private sectors that are required to or are seeking to evaluate their cyber security posture, identify vulnerabilities, assess risks, and ensure compliance with applicable regulatory standards and industry best practices.

5. Definitions

i. **Cyber Security Audit** - A systematic and independent assessment of an organization's security controls, policies, and procedures to evaluate their effectiveness in protecting information systems and data from cyber threats.

ii. **Scope of Audit** – The defined parameters of an audit engagement, specifying the systems, functions, departments, assets, and processes to be evaluated.

iii. **Audit Evidence** – Any information, documentation, logs, observations, or other forms of data collected during the audit that substantiate audit findings and support conclusions. Audit evidence must be accurate, relevant, and sufficient to validate the audit's objectives and must be properly documented and appended to the audit report.

iv. **Working Notes** – Internal documentation created and maintained by auditors during the audit process, capturing audit activities, methodologies employed, evidence gathered, and preliminary findings. These notes serve as a record to substantiate conclusions and facilitate subsequent review and verification. The Auditing organization to ensure adherence to "Policy Guidelines for Handling Audit related Data" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Policy_Guidelines_Handling.pdf)

v. **Observation** – A documented finding resulting from the audit process, identifying either conformity or deviations from established controls, standards, or procedures. Observations are supported by objective, verifiable evidence and may indicate potential areas of improvement or non-compliance.

vi. **Non-Conformity / Non-Compliance** – A condition wherein a process, control, or practice fails to meet the prescribed standards, regulatory requirements, or internal policies. Non-conformities may indicate gaps or weaknesses in the control environment that require corrective action.

vii. **Root Cause Analysis (RCA)** – A systematic investigative process used to identify the fundamental causes or underlying factors that contribute to an incident, audit finding, or failure. RCA seeks to address the source of the issue rather than merely its symptoms to ensure effective corrective actions.

viii. **Closure Report** – A comprehensive report generated at the conclusion of the audit, indicating that all audit observations, findings, and issues have been addressed, remediated, or closed. The closure report confirms that the audit engagement has met its objectives and that all necessary corrective actions have been taken.

ix. **Threat** – A potential event or condition that could exploit a vulnerability and result in harm, disruption, or damage to a system, organization, or its assets. Threats may be natural, technological, or human in nature.

x. **Risk** – The probability and impact of a threat exploiting a vulnerability, often quantified as the likelihood of occurrence and the severity of potential consequences. Risk assessment typically involves evaluating the combination of threat likelihood and the magnitude of impact to determine the risk level.

xi. **Security Posture** – The overall security standing of an organization's information systems, networks, and associated controls at a specific point in time. This posture reflects the organization's ability to prevent, detect, and respond to security incidents effectively.

xii. **Control or Security Control** – A measure, safeguard, or countermeasure implemented to mitigate risk, enforce security policies, and protect the confidentiality, integrity, and availability of systems, data, and assets. Controls may be administrative, technical, or physical in nature, and are designed to reduce vulnerabilities and prevent threats from exploiting them.

xiii. **Network Infrastructure** – The collection of physical and virtual components, including but not limited to routers, switches, firewalls, communication cables, and associated software, that enable data transmission and ensure the security and reliability of network operations within an organization.

xiv. **Staging Environment** – A non-production, controlled environment that replicates the production environment, where applications, software, or system configurations are thoroughly tested and validated prior to deployment in the live, operational environment.

xv. **Production Environment** – The live, operational setting where the organization's systems, applications, and services are actively used by end-users.

xvi. **Non-Disclosure Agreement (NDA)** – A legally binding contract between parties, obligating confidentiality regarding sensitive or proprietary information exchanged during the audit engagement. The NDA ensures that audit-related data, findings, and communications remain confidential and are not disclosed without proper authorization.

xvii. **Conflict of Interest** – A situation in which an auditor's personal, financial, or organizational interests may influence or compromise their ability to conduct the audit in an objective and impartial manner. Such conflicts must be disclosed and managed to maintain the integrity and credibility of

the audit process. This includes scenarios where the same entity is involved in both the implementation of controls and their subsequent audit, or in conducting audits while also being responsible for remediation activities. Such overlaps create inherent conflicts that undermine the independence of the audit process. All such conflicts must be disclosed and managed to maintain the integrity and credibility of the audit process.

xviii. **Common Vulnerabilities and Exposures (CVE)** – A publicly disclosed, standardized list of unique identifiers assigned to known cyber security vulnerabilities. Each CVE entry contains a distinct identifier, a brief description of the vulnerability, and references to additional resources. CVE serves as a common language for tracking and sharing information about vulnerabilities across various platforms and organizations.

xix. **Common Weakness Enumeration (CWE)** – A community-developed, list of common software and hardware weaknesses that may lead to security vulnerabilities. A "weakness" refers to an inherent flaw or condition within software, firmware, hardware, or services that, under specific conditions, may introduce risks or vulnerabilities.

xx. **Denial of Service (DoS) & Distributed Denial of Service (DDoS) Testing** – A simulated attack on a system designed to assess its capacity to withstand traffic overloads or service disruptions. DoS and DDoS testing measure the resilience of systems to prevent downtime and maintain service availability during high-volume and malicious traffic events.

xxi. **Vulnerability Assessments**- Examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of

proposed security measures, and confirm the adequacy of such measures after implementation.

xxii. **Penetration Testing**- A security testing methodology in which individual components or the application as a whole are actively tested to identify and exploit potential vulnerabilities. The objective is to determine whether these vulnerabilities can be exploited to compromise the application, access sensitive data, or affect the underlying infrastructure and environment.

xxiii. **Red Team Assessment**- An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

xxiv. **Classification of vulnerabilities based on Severity:** In cybersecurity audits and vulnerability assessments, it is crucial to classify vulnerabilities based on their severity to determine appropriate remediation priorities. Two widely adopted frameworks for assessing and classifying severity are:

- CVSS: The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. It provides a score from 0.0 to 10.0, helping stakeholders understand the risk level and prioritize remediation.
- EPSS: The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. The EPSS model produces a

probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

Auditors are required to implement both CVSS and Exploit Prediction Scoring System (EPSS) frameworks within their audit reports. The observations/vulnerabilities in the report must be categorized based on the Common Vulnerability Scoring System (CVSS) for severity and supplemented with the Exploit Prediction Scoring System (EPSS) to assess the likelihood of real-world exploitation.

6. Scope of Engagements Covered

The types of cyber security audits and assessments including, but not limited to, those listed below, may be carried out and fall within the scope of this document. Auditee organizations, which are expected to ensure a comprehensive audit covering all aspects of their Information and Communication Technology (ICT) systems at least once a year, may also opt for additional assessments and audits during the year.

i. Compliance Audits- Evaluation of an organization's security practices to ensure they adhere to relevant industry standards, regulations, and policies.

ii. Risk Assessments- The process of identifying and evaluating risks arising from cyber threats, vulnerabilities, and potential cyberattacks that could impact organizational operations, organizational assets, individuals, and connected entities. This involves assessing the likelihood and impact of various cybersecurity incidents.

iii. Vulnerability Assessments- Examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

iv. Penetration Testing- A security testing methodology in which individual components or the application as a whole are actively tested to identify and exploit potential vulnerabilities. The objective is to determine whether these vulnerabilities can be exploited to compromise the application, access sensitive data, or affect the underlying infrastructure and environment.

v. Network infrastructure Audits- Comprehensive review of network components, including hardware devices such as firewall, end point

devices, servers, router, network switches, IPS / IDS etc., software, configurations, access controls, and security measures, to identify vulnerabilities, inefficiencies, and areas for improvement.

vi. Operational Audits- Evaluation of an organization's cyber security operations, processes, and controls to assess their efficiency, effectiveness, and alignment with security objectives.

vii. IT security policy review and assessment against security best practices.

viii. Information Security Testing- The process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements.

ix. Source Code Review- Examining an application's source code to identify security vulnerabilities, coding errors, and inefficiencies, ensuring adherence to best practices, coding standards, and regulatory requirements to improve code quality and security.

x. Process Security Testing- Evaluating the security measures and controls within an organization's operational processes to identify vulnerabilities and ensure that sensitive information, systems, and applications are protected from security threats.

xi. Communications Security Testing- Evaluating the security measures implemented on communication channels to identify vulnerabilities and ensure that information transmitted over those channels is protected from unauthorized access, interception, modification, or disruption

xii. Application security testing (including web applications, mobile applications and APIs)- Assessing an application's architecture, components, and configuration to identify security vulnerabilities.

xiii. Mobile Application Security Auditing – A structured evaluation of mobile apps to identify security vulnerabilities, assess data protection, and ensure

compliance with secure development practices.

xiv. Wireless Security Testing- Evaluating the security measures of a wireless network by simulating attacks to identify potential vulnerabilities and ensure the network is protected against unauthorized access and data breaches

xv. Physical Security Testing- assessing and evaluating the physical security measures that protect an organization's assets, including its facilities, equipment, and personnel, from unauthorized access, theft, damage, or other physical threats.

xvi. Red Team Assessment- An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

xvii. Digital Forensic Readiness Assessment- Evaluating an organization's preparedness to effectively collect, preserve, and analyze digital evidence in the event of a security incident.

xviii. Cloud Security Testing- Evaluating and assessing the security measures, configurations, and vulnerabilities of cloud-based systems, applications, and infrastructures

xix. Industrial Control Systems/ Operational Technology Security Testing- Evaluating the cyber security posture of industrial control systems (ICS) and operational technology (OT) networks, specifically designed to identify vulnerabilities and potential threats that could disrupt critical industrial processes, impacting safety, production, and overall system availability within a facility.

xx. Internet of Things (IOT)/ Industrial Internet of Things Security Testing (IIOT)-Evaluating and validating the security posture of connected devices within an IoT network, particularly in industrial settings, by identifying vulnerabilities and potential attack vectors.

xxi. Log Management and Maintenance Audit-Assessing the effectiveness and completeness of system and security log generation, retention, integrity, and monitoring practices, ensuring that logs are maintained in accordance with organizational policies and regulatory requirements to support detection, investigation, and response activities.

xxii. Endpoint Security Assessment-Evaluating the security posture of endpoint devices (e.g., desktops, laptops, mobile devices) by assessing configurations, patching, malware protection, encryption, access controls, and monitoring mechanisms to ensure robust protection against endpoint-based threats.

xxiii. Artificial Intelligence (AI) System Audits – Evaluation of AI systems for security, ethical alignment, transparency, data integrity, and resilience to adversarial manipulation.

xxiv. Vendor Risk Management Audits – Assessment of third-party and vendor cybersecurity practices to identify supply chain risks and ensure alignment with organizational security policies.

xxv. Blockchain Security Audit – A structured assessment of blockchain systems, including smart contracts and infrastructure, to identify vulnerabilities, verify cryptographic integrity, evaluate access controls and consensus mechanisms, and ensure compliance with security best practices and regulatory requirements.

xxvi. SBOM (Software Bill of Materials), QBOM (Quantum Bill of Materials), and AIBOM (Artificial Intelligence Bill of Materials) Auditing – Evaluation of the Software Bill of Materials (SBOM), Quantum Bill of Materials (QBOM), and Artificial Intelligence Bill of Materials (AIBOM) to ensure transparency, traceability, and integrity of components used in software, quantum computing, and AI systems. This audit focuses on identifying known

vulnerabilities, licensing issues, and supply chain risks associated with open-source and third-party components, and verifies adherence to secure development lifecycle practices and regulatory compliance.

7. Basic principles in Audit

The effectiveness of a cyber security audit relies on the adherence to fundamental principles that guide the auditor's conduct, ensuring that the audit process is thorough, unbiased, and meets established standards of quality. The following basic principles serve as the foundation of the audit methodology outlined in this document:

i. **Independence**

Auditors must remain free from bias, conflict of interest, and external influence. Audit findings must be based solely on evidence. To ensure the audit assessment remains objective and free from undue influence, the commercial arrangements between the auditee and the auditing organization must be structured to maintain independence. Especifically, payments to the auditing organization should not be contingent upon the outcome of the audit—whether favorable or unfavorable—nor should they be tied to the submission or approval of any closure reports. Linking payments to audit outcomes or closure status could compromise the impartiality of the assessment and create a conflict of interest. It is recommended that auditing fees be based on predefined scopes, deliverables, and timelines, and not influenced by the findings or the post-audit compliance status of the auditee.

In case the auditing organization faces any pressure tactics, coercion, or undue influence from the auditee that may compromise the independence of the audit, the matter should be promptly escalated to CERT-In for appropriate intervention and resolution.

ii. **Objectivity**

Objectivity refers to the auditor's duty to maintain impartiality and fairness throughout the audit. Auditors must avoid situations that could impair their ability to form unbiased judgments. This includes refraining from accepting gifts, favours, or any other benefits that may influence the audit outcome. The auditor's objective is to present findings and conclusions that are supported by verifiable evidence, without being swayed by external pressures or personal preferences.

iii. **Integrity**

Integrity is fundamental to the audit process. Auditors must act honestly and with strong ethical principles, maintaining a high standard of conduct even in the face of challenges. Integrity also entails a commitment to providing clear, accurate, and truthful reports, reflecting the true state of the auditee's cyber security posture.

iv. **Professional Skepticism**

Auditors should critically assess information, question assumptions, and seek supporting evidence to identify gaps, inaccuracies, or risks not immediately visible.

v. **Professional Judgment**

Informed decisions must be made using experience, evidence, and contextual understanding of the auditee's environment, risk profile, and regulatory requirements.

vi. **Professional Care**

Audits should be performed with diligence, competence, and attention to detail. Auditors must stay updated with evolving threats and follow relevant standards and best practices. Auditors must ensure that their work is

conducted in a manner that meets or exceeds the professional standards required for the engagement.

vii. **Confidentiality**

Throughout the audit process, auditors must protect the privacy and integrity of the information to which they have access, ensuring it is not disclosed without proper authorization. The Auditing organization to ensure adherence to “Policy Guidelines for Handling Audit related Data” published on CERT-In’s website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Policy_Guidelines_Handling.pdf)

viii. **Transparency and Accountability**

Audit processes, methods, and conclusions should be clearly documented and communicated. Auditors are responsible for ensuring the credibility and reliability of their work.

By adhering to these basic principles, auditors ensure that cyber security audits are conducted with the highest standards of professionalism, rigor, and impartiality without any pressure from the auditee organizations and other stakeholders. These principles not only enhance the credibility of the audit process but also help build trust between the auditing organization, the auditee, and other stakeholders.

8. Applicable standards and Frameworks

i. Auditing organization must utilize industry standard methodologies, best practices for security testing. Solely tools-based testing should be discouraged as tool-based audits may focus primarily on automated processes and may overlook non-automated or manual components of the IT infrastructure. This limitation can result in an incomplete view of the overall security.

ii. The limited lists such as OWASP Top 10, SANS Top 25 and similar, should not be considered as standards or references for audits. Instead, audits should include discovery of all known vulnerabilities based on the comprehensive standards/frameworks like ISO/IEC, Cyber Security Audit Baseline Requirements, CSA Cloud Controls Matrix (CCM) for Cloud Security, Open Source Security Testing Methodology Manual (OSSTMM3), OWASP Web Security Testing Guide for web application security testing, OWASP Application Security Verification Standard (ASVS) for establishing and verifying application security controls, the OWASP Mobile Security Testing Guide (MSTG) for mobile app audits OWASP DevSecOps Maturity Model for assessing Continuous Integration / Continuous Deployment (CI/CD) pipeline security along with applicable regulatory framework and directions & guidelines issued from time to time by agencies such as CERT-In, Government and regulatory bodies.

iii. 'Cyber Security Audit Baseline Requirements' document published on CERT-In's Website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf) should be used by auditees and auditing organizations to build their audit program.

iv. Guidelines and directions issued by CERT-In and regulators to be included as part of scope of audit by default.

v. **For audits of critical Applications/databases/platform of Ministries, Departments, Secretariats, and Offices, wherever sensitive Personal identifiable information (PII) data is involved, the auditing organization shall verify compliance with the "Comprehensive Audit Program Checklist – Cyber and Information Security Audit" as outlined in the "Guidelines on Mandatory Features of Cybersecurity Architecture to be Ensured in all Ministries/Departments" issued by the Cyber Security Division, Ministry of Electronics and Information Technology. This checklist, comprising 282 control points, shall form the default mandatory audit scope for such entities and must be thoroughly assessed during the audit process.**

vi. Auditing organization must verify the existing policies of the organization against the industry standards and best practices and suggest the necessary improvements, if required.

vii. Auditee organizations must confirm that applications are designed & developed with secure practice prior to commencing any assessment. Organization should incorporate secured application development practices and application owners should ask for adherence to the best practices highlighted in the document "Guidelines for Secure Application Design, Development, Implementation & Operations" published on CERT-In's Website. (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf).

viii. Application developed without any secure design and development practices should not be considered for assessment and audits. The same

should be informed to the auditee organization in writing with a copy marked to CERT-In. Auditee organizations and auditor organizations must confirm that application is designed & developed with secure practice prior to commencing any assessment.

ix. The auditing process should be viewed as a tool for the continual process improvement of the auditee organization's security posture, rather than a mere formality for compliance. Audits must not be conducted solely for the sake of fulfilling regulatory requirements; instead, they should adopt a risk-based and domain-specific approach that aligns with the organization's business context, threat landscape, and operational priorities. The auditor's perspective should be focused on identifying meaningful gaps, refining security processes, and recommending practical, actionable improvements. Further, audit findings and recommendations should be clearly articulated in language that is understandable to executive leadership and decision-makers, enabling informed risk management and strategic decision-making.

9. Auditee Responsibility

9.1 Governance and Oversight by Top Management

i. Top management should review & approve the audit program, scope and remedial measures taken by organization to plug the vulnerabilities highlighted in the audits in a time bound manner.

ii. While cyber security audits are essential for identifying vulnerabilities, assessing risks, and ensuring compliance with security standards, the responsibility for maintaining an efficient and robust cyber security posture ultimately rests with the auditee organization, not the auditor.

iii. The frequency and broad scope of audits should be included in the annual reports. However, these reports should exclude any confidential details, infrastructure or application specifics, vulnerabilities, or related observations.

iv. Auditee organizations should follow cyber security auditing related advisories and directions issued by CERT-In.

9.2 Risk Acceptance and Exception Handling

i. Risk treatment techniques such as retain, avoid, transfer and reduce for any reported vulnerabilities or observations in the application or infrastructure, must be authorized & accepted by the head of the auditee organization.

ii. Any exceptions to reported vulnerabilities or observations in the application must be authorized by the head of the organization, who is the owner of the application.

9.3 Remediation and Follow-up

i. After receiving audit findings, the auditee is responsible for implementing the recommended actions to improve security and mitigate risks.

ii. The auditee organization must act upon the relevant audit findings and strive to improve the IT security.

iii. Vulnerabilities highlighted in audit reports should be patched by owners/developer at the earliest. The responsibility of patching and correction of vulnerabilities is the responsibility of Auditee organization.

iv. Follow-up audits should be included within the scope or RFP proposal and must be conducted by the auditing organization after the closure of vulnerabilities or issues identified during the initial audit.

9.4 Internal Monitoring and Development Practices

i. Continuous internal audits/assessments should be carried out by auditee entities and they are expected to ensure that the necessary competencies and skill sets (including relevant professional experience and qualifications) are available to undertake internal audits/assessments.

ii. Auditee organizations must ensure that 'Secure by Design' principles and secure application development practices are included as mandatory requirements in their RFPs and tenders for application/software development.

9.5 Application Handling and Audit Artifacts

i. The application developer should avoid making any code changes to the audited application or infrastructure, after issuance of the audit certificate. It is recommended that audit-related artifacts, such as

hash values, versions, and timestamps, be captured by the auditee organization and shared with the auditing organization. These details should be prominently featured in the audit certificate and reports.

ii. Version control and change management be effectively implemented so that the assets that were/are part of audit scope can be backtracked.

iii. The audit reports shall be signed only by the manpower declared to CERT-In, as listed in the organization's snapshot information available on the CERT-In website. The report must be signed by the Auditors who conducted the audit. It should then be reviewed and signed by a designated Reviewer who is not part of audit team and is from mid-management, to ensure an unbiased and quality review. Finally, the report must be authorized and signed by the Head of the Auditing Organization (e.g., Director, Partner, or CEO), certifying the completeness, accuracy, and integrity of the audit findings and recommendations. The audit certificate must be signed by both the Lead Auditor and the Head of the Auditing Organization.

9.6 Asset Management and Infrastructure Security

i. The complete audit process of the information infrastructure must be undertaken up by the auditee organization itself, except in cases where there is a specific mandate from a Regulator, Government, or relevant stakeholder. Accordingly, the entire process — from defining the audit scope, selecting the auditing organization, providing access to the information infrastructure, to ensuring closure of all audit observations — must be carried out by the owner of the information infrastructure. This responsibility must not be delegated. However, the organization may seek external support for specialized expertise,

while retaining full ownership and accountability for the security of its information infrastructure.

ii. Organizations should maintain and monitor the inventory of all the authorized assets (both software and hardware). For all the assets, proper patch management mechanism should be in-place to patch the vulnerable software, applications and firmware used by the organization.

iii. Organizations should have secure configuration of assets. Appropriate security measures, such as blocking of unused ports, securing and changing default settings and credentials should be implemented during deployment of equipment and applications.

iv. Organizations need to implement the principle of least privilege across the organization's assets. This means that users, systems, applications, and processes should be granted only the minimum level of access permissions necessary to perform their specific roles or function. This limits the potential impact of security breaches, reduces insider threats.

v. Ensure restricted remote access to the cyber infrastructure. Remote access traffic should be tunneled, encrypted and logged to avoid any misuse. Multi Factor Authentication (MFA) is mandatory for remote access of the cyber infrastructure.

vi. Organizations should only use genuine software in their infrastructure and ensure to update software, application and firmware on regular basis to avoid software vulnerabilities. Organizations should also ensure to use secure protocols over weak vulnerable protocols to avoid vulnerabilities associated with weak protocols.

vii. During onboarding, the auditing organization should deliver a presentation to the auditee organization's Board and senior management, explaining their understanding of the audit scope, the methodology to be adopted, and the associated timelines. Similarly, during the exit conference, the auditing organization should present key findings, highlight the overall security posture, and outline associated risks to support informed decision-making.

10. Auditor Responsibility

10.1 Role and Accountability of the Auditor

i. Auditing serves as an independent assessment of an organization's security practices, systems, and controls. The auditor's role is to evaluate the effectiveness of these measures, verify compliance with relevant standards and regulations, and provide recommendations for improvement. However, the auditor is not responsible for managing or maintaining the organization's security measures directly or indirectly; their responsibility is limited to reviewing and reporting on the state of security at the point in time of the audit.

ii. If any of the assets included in the audit scope are found to be inaccessible during the audit, the auditing organization must promptly inform the auditee and request resolution of the accessibility issues. If the auditee organization is unable to resolve the issues, the affected assets must be explicitly mentioned in the audit report, along with the reasons for their exclusion from the audit and same must be brought to the notice of CERT-In.

10.2 Auditor Personnel: Conduct and Competency

i. During and after the audit assignment, personnel involved must be aware of information classification requirements and adhere to practices that ensure the confidentiality, security, and privacy of information. This includes, but is not limited to, the proper collection, use, disclosure, and protection of information, as well as safeguarding it against theft, loss, or damage.

ii. All audit team members must have a valid Non-Disclosure Agreement (NDA) in place with their employer organization.

Additionally, depending on the specific project requirements, they may also be required to sign a separate NDA with the auditee organization, with the employer organization being duly informed of such an arrangement.

iii. The resources must understand and ensure there is no conflict of interest.

iv. The resources must have experience and maturity in interacting with senior management and creating trust.

v. The resources must have adequate competency in:
   a. Security Technologies
   b. Security Processes
   c. Security Controls
   d. Security Trends
   e. Fact Collection
   f. Reporting

vi. Auditing Organization must only deploy manpower declared to CERT-In in Snapshot Information Form published on CERT-In's website(https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Empanel_org.pdf).

vii. The resources should be courteous, cooperative, and professional.

viii. The resources should demonstrate high standards of ethical practices and professional conduct.

ix. The resources should understand the consequences of their actions.

x. A continuous capacity-building program for both technical staff and senior management of the auditing organization should be

developed and maintained, focusing on emerging domains and technologies.

10.3 Handling Audit related data:

i. The auditing organization should treat audit-related data as confidential, handle it with due diligence, and protect it from access by temporary staff or staff in transition/retirement. The auditing organization should immediately implement strict access control for any staff in transition, and the auditee should be apprised of any change in this regard.

ii. Auditee related data should be stored only on systems located in India with adequate safeguards and should keep the auditee informed of the means & location of storage and seek Auditee's consent, where necessary.

iii. During project engagement, Audit related data should be kept in encrypted form in Auditor's laptop.

iv. Auditing organization should also ensure that data is wiped from auditor's laptop after completion of the project. After wiping the data, auditing organization should also make sure that data cannot be retrieved by any known forensic technique. A certificate to this effect should be formally issued to the auditee organization, confirming that all audit-related data has been permanently and irreversibly deleted in accordance with secure data disposal practices.

v. The Auditing organization may retain the audit reports with adequate safeguards to ensure integrity and confidentiality, after completion of audit and it can be shared on 'need to know basis' with the relevant stakeholders after seeking approval from auditee

organization, when required. The data retained should not include any auditee data other than the audit reports.

vi. Auditee related data should only be retained for specific period of time as in Agreement with the auditee or the guidelines by Regulator and disposed-off as per defined & agreed process. The collection, preservation and disposal of data collected by the auditor should be in accordance with the Agreement entered between Auditor & Auditee. In case no specific period is mentioned in Agreement, the data should be retained by auditing organization for 1 year from completion of project.

vii. The Auditing organization to ensure adherence to "Policy Guidelines for Handling Audit related Data" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Policy_Guidelines_Handling.pdf).

viii. Audit report should be clear, precise and comprehensive to include all details of audit process, detailed scope, duration of audit, methodologies/standard used, tools, manual process, findings, prioritization, sampling decisions, manpower involved, exemptions, limitations and other constraints

ix. The audit reports shall be signed only by the manpower declared to CERT-In, as listed in the organization's snapshot information available on the CERT-In website. The report must be signed by the Auditors who conducted the audit. It should then be reviewed and signed by a designated Reviewer who is not part of audit team and is from mid-management, to ensure an unbiased and quality review. Finally, the report must be authorized and signed by the Head of the

Auditing Organization (e.g., Director, Partner, or CEO), certifying the completeness, accuracy, and integrity of the audit findings and recommendations.

10.4 Awareness, Training and Outreach

i. Auditing organizations should arrange in-person sessions for their clients or targeted sector on audit awareness, covering the audit fundamentals of cyber security audits such as audit scope, outcomes, limitations of audits, secure development practices and CERT-In initiatives, directions & guidelines on cyber security.

ii. The Auditing organization must maintain a professional relationship with the auditee organization even after the completion of the audit process to keep auditee organization updated for the latest security developments and to help in implementing the secure environment.

10.5 CERT-In Affiliation and Branding Compliance

i. Ensure that CERT-In is not made or projected to be a part of any contract between auditee and auditing organization.

ii. Auditing organization shall not use the CERT-In logo, nor make any reference to the Auditors association with CERT-In on any publicity material, promotional material or product without the prior written permission of CERT-In. Before CERT-In examines requests for permission, the Auditing organization shall submit the wording and presentation of such information.

iii. Auditing organization may use the words “This Organization is empaneled by CERT-In for providing information Security Auditing Service”. No other words shall be used to describe the Auditing organization’s relationship with CERT-In without the prior written permission of CERT-In.

iv. It is responsibility of empaneled organization to keep CERT-In updated with Snapshot and Point of Contact (PoC) information.

v. Auditing organizations should share the information about their cyber security initiatives with CERT-In for value addition and disseminate it to boarder community.

vi. The Auditing organization shall indemnify, and keep indemnified CERT-In against all claims, demands, actions, costs, expenses, (including without limitation, damages for any loss of business, business interruption, loss of business information or other indirect loss), arising from or incurred by reason of any third party claims against CERT-In relating to or arising from the performance or non-performance by the Auditing organization of any or all of its obligations under this terms and conditions, as well as its Contract with the auditee.

vii. Empaneled organization should not engage in activities like digital break-in, sub-letting or outsourcing of audit assignment, violating terms & conditions of empanelment and unethical business transactions.

10.6 Sharing of Audit report and Audit metadata with CERT-In

It is mandatory for the auditing organization to provide the information pertaining to audits carried by them to CERT-In within 5 days of completion of audit as per format prescribed by CERT-In from time to time to enable CERT-In to act in the matter(s) of capacity building, audit framework, benchmark, quality control and others measures as may be required. The audit data submitted by the entities will be kept confidential.

11. Quality control of auditing organisations involved in Audit

i. CERT-In at any point in time can be a part of the audit team of the auditing organization to assess the quality and maturity of audit and the same should be communicated clearly in writing to the auditee by the auditing organization.

ii. CERT-In reserves the right to seek/audit information from auditing organizations for any project done within the time frame of the empanelment period.

iii. Auditee organization to provide feedback on the audit conducted to CERT-In as well as to auditing organization on completion of the audit. Feedback/complaints to CERT-In would help improve the quality of selecting auditing organizations in future. It is both an auditee organization's right and duty to provide relevant feedbacks. All feedback/complaints are kept confidential and are acted upon promptly with utmost importance. Auditee Feedback form may be requested from empanelment@cert-in.org.in

iv. In case of any adverse feedback from auditee organization/ agencies or any lapses in audit assignments are observed by / reported to CERT-In, actions as per Deter and Punish Framework published by CERT-In (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In >https://www.certin.org.in/PDF/RoD_Interaction_session_website.pdf) may be taken without any reminder or notice.

v. To ensure the quality of audits, auditee organizations are advised to follow practices detailed under Section 12: "Selection of Auditor".

12. Selection of Auditor

12.1 Utilizing Snapshot information for Shortlisting Auditing Organizations

i. The snapshot information of skills and competence of CERT-In empaneled auditing organizations published on CERT-In's website should be utilized by the organizations or sectoral regulators to identify and select the auditing organizations by mapping their requirements with the competence of auditing organizations.

ii. Information about the CERT-In empaneled auditing organizations is available at CERT-In website. The information provided on the CERT-In website can help the auditee organization with respect to the following:

a. Evaluation of manpower and skillset details of an auditing organization.

b. Experience of an auditing organisation relevant to information security audits.
Categories of information security audit conducted by the auditing organization.

c. Information security audits carried out by an organization in last 12 months (sector-wise).

d. Category-wise number of audits conducted by an organization in last 12 months based on data provided by the auditee organization.

e. Technical manpower deployed for audits by an organization with details.

f. Tools used in various audit.

12.2 Selection Process and Evaluation by Auditee

i. The Auditee organizations should interview and select the resources aligned by auditing organizations for competency and experience with respect to the scope of Audit.

ii. Auditee organizations need to verify the technical credentials of the manpower deployed for the audit at their end in line with the qualification requirement mentioned at "Guidelines for applying for Empanelment" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/InfoSecAuditorsEmpGuidelines.pdf).

iii. Auditee organizations must verify the identity, official identity cards/ government issued documents and designations of the auditing team to ensure that the individuals conducting the audit are legitimate and authorized. Auditing organizations should not field freelancers, interns, freshers, moonlighters, third party consultant or employees who are serving their notice period and the auditee organizations should verify compliance.

iv. While selecting an auditing organization, it is the responsibility of the auditee organization to check the domain of audit conducted, previous audits conducted and other relevant details. Auditee organization should have a clear understanding of the auditing organization's audit methodology, tools used, experience in the relevant domain and all available alternatives like other competent organizations before selecting.

12.3 Resource Vetting and Deployment Standards

i. The resources must have undergone a background check before employment by the auditing organizations. In case of employees moving from one CERT-In empaneled organization to another, a NOC / Relieving Letter shall be required from the previous organization as part of background check and revised snapshot information has to be communicated to CERT-In.

ii. Background verification of individual auditors/employees is the sole responsibility of the auditing organizations. The auditing organization is required to conduct background checks both prior to and, if necessary, following employment.

iii. Auditing Organization must only deploy manpower declared to CERT-In in Snapshot Information Form published on CERT-In's website(https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Empanel_org.pdf). CERT-In reserves the right to verify/audit such information independently or from the auditing organization or the auditee organization.

12.4 Contractual Guidelines and Contingencies

i. Contracts for the audit of applications especially those are critical or have high user reach, should be awarded by auditee organizations for a period of 2–3 years to enable continuous audits at a defined frequency.

ii. If the credibility of the auditing organization is unclear, auditee organization must make sure that the contractual agreement allows the auditee organization to stop the audit and choose

another auditing organization within a reasonable duration of time in order to avoid financial losses on both ends.

13. Planning the Audit

13.1 Guidelines for Auditee Organizations

13.1.1 Defining and finalizing audit scope

Below mentioned points must be taken into consideration while finalizing the scope of Audit:

a) The auditee organisation should define the complete and comprehensive scope for the audit. The scope of audits should include audit of entire cyber infrastructure including system, applications (both Web/Mobile), software, network infrastructure, Operational Technology (OT) / Industrial Control Systems (ICS) environment, cloud architecture, Application Programming Interfaces (APIs), database and hosting infrastructure, code review, application security, data Security, testing of Incident response capability of the auditee.

b) Scope of audit should be clearly defined by auditee organization in consultation with auditing organization.

c) The scope must be derived from the consolidated and updated asset inventory of the organization. The asset inventory should be reviewed and updated periodically by the IT team.

d) The scope to be submitted to the auditing organisation must be vetted by the internal audit team in consultation with CISO.

e) The auditee organization should provide a comprehensive scope for the audit, ensuring that assets related to the testing / UAT, development, and production environments are included to achieve complete audit coverage.

f) Third-party risk assessment/vendor risk assessment /supply chain risk assessment should be part of scope.

g) The scope of work should clearly specify the requirement to conduct follow-up audits as part of the engagement.

13.1.2 Audit Frequency and Trigger Conditions

i. The cyber security audit should be conducted at least once in a year. The sectoral regulators may decide to increase the audit frequency based on the size of the organization, the criticality of the assets being audited and the complexity of the adoption of digital infrastructure etc.

ii. The above-mentioned frequency may be treated as the minimum frequency and organizations may opt to conduct audits more frequently depending on its risk appetite and criticality of operations and assets.

iii. All changes to the system or application must undergo a formal change management process. Each change should be classified as either a 'Minor Change' or a 'Major Change'. Minor change (low-risk, non-critical) require standard change management processes but do not need a cyber security audit. Major change (high-risk, impactful to security) such as system overhauls, technology migrations, or configuration adjustments that affect sensitive data or critical infrastructure must undergo a cyber security audit to evaluate potential vulnerabilities, ensure compliance, and mitigate security risks before implementation.

iv. Audit should be performed after every major change in infrastructure and application, based on the criticality involved.

v. Audits should be performed even if there is no major change in infrastructure at periodic interval of time to remediate and eliminate the risk from new vulnerabilities. Periodicity of audits should be decided based on the criticality of cyber assets.

13.1.3 Identification and Inclusion of Critical Assets

i. The critical databases/applications need to be identified by the auditee organizations and it must be ensured that the identified critical databases/applications are included in the scope of cyber security audits.

ii. For the identified critical databases, the information security audit should include, but not limited to, database configuration audit.

iii. For the identified critical applications, the information security audit should include, but not limited to, DAST (Dynamic Application Security Testing) and SAST (Static Application Security Testing). Additionally, when procuring the application, the auditee organizations should require that the software developer and/or system integrator supplying the software, perform Static Application Security Testing (SAST). This requirement should be clearly stated in the RFPs and tenders.

13.1.4 Audit Team Planning and Stakeholder Coordination

i. In case any of the activities to be audited in the auditee organization are outsourced, auditee organization must ensure that relevant personnel from outsourced organization are available at the time of audit. The auditing organization's responsibilities need to articulate not just the audit tasks, but also the documentation of their activities, reporting their actions and modus operandi.

ii. A Technical team should be assigned as point of contact by the auditee organization for assisting and monitoring the auditing organization during the audit and the details of the technical team should be shared with the concerned auditors. Auditee organization should assure and schedule regular interaction of technical team with auditors.

13.1.5 Planning for Hosted and Third-Party Infrastructure

i. In cases where a service or website is hosted on a web server owned by another organization, the responsibility for information security auditing of the web server, its operating system, the web hosting application software, and any backend database application software lies with the organization that owns and operates the server, as the website content owner does not have access to or control over these assets. However, since the data and software related to the website are managed by the organization owning the website content, it is their responsibility to ensure that these components are audited by a CERT-In empaneled information security auditing organization.

ii. The organization owning the website content may select any auditing organization from the list of CERT-In empaneled information security auditing organizations, in accordance with its internal rules, procedures, and financial guidelines, to carry out the audit. The audit report provided by the selected auditing organization should explicitly certify that the audited web application including backend databases and scripts, if any, are free from vulnerabilities and malicious code that could be exploited to compromise or gain unauthorized access, including escalated privileges, to the web server hosting the website.

13.1.6 Secure Handling of Reports and Data

A well-defined mechanism must be in place which clearly states the procedure in which the report would be stored and destroyed after the completion of audit by the auditing organization. Thus, the mechanism should be designed in such a way that it confirms the following:

a) Secure handling of report and data at transit.
b) Secure handling of report and data at rest.
c) Disposal time of report and related information by auditing organization.

13.1.7 Audit Contracts, Agreements and Governance

i. The contract should include clear identification of the following:
   a) Audit criteria and standard (Mutually agreed upon by the parties) to discovery all known vulnerabilities based on the comprehensive standards/frameworks like ISO/IEC, Cyber Security Audit Baseline Requirements, CSA Cloud Controls Matrix (CCM) for Cloud Security, Open Source Security Testing Methodology Manual (OSSTMM3), OWASP Web Security Testing Guide for web application security testing, OWASP Application Security Verification Standard (ASVS) for establishing and verifying application security controls, the OWASP Mobile Security Testing Guide (MSTG) for mobile app audits OWASP DevSecOps Maturity Model for assessing CI/CD pipeline security along with applicable regulatory framework and directions & guidelines issued from time to time by agencies such as CERT-In, Government and regulatory bodies.
   b) Audit plan with timelines (Mutually agreed upon by the parties).
   c) Audit tasks.

d) Documentation requirements.

e) Audit Support requirements.

f) Reporting Requirements: Structure, content and secure handling of final deliverable (such as audit reports) should be mutually agreed by auditee and auditing organization.

g) The clause to revalidate the audit observations after the compliance window mentioned in the IS audit policy of the respective auditee organization.

ii. A Non-Disclosure Agreement (NDA) must be signed by the Information Security Auditing Organization prior to the commencement of any audit activities. The auditing organization and its auditors are ethically and contractually obligated to maintain the confidentiality of the auditee's information and security testing results. NDA template is available at CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/NON-Disclosure_Agreement.pdf). In addition to the NDA, if the auditee organization wishes to incorporate provisions addressing penal & legal liabilities, such clauses may be included directly in the contract between the auditee and the auditing organization, and may also extend to individual auditors responsible for conducting the audit.

iii. Escalation Matrix should be defined as part of Audit contract in case of repeated vulnerabilities.

13.1.8 Reference Standards and Initial Guidelines

i. 'Cyber Security Audit Baseline Requirements' document published on CERT-In's Website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-

in.org.in/PDF/CyberSecurityAuditbaseline.pdf) should be used by auditees and auditing organizations to build their audit program.

ii. Guidelines and directions issued by CERT-In and regulators to be included as part of scope of audit by default.

13.2 Guidelines for Auditing Organizations

13.2.1 Planning Legal and Confidentiality Requirements

i. Ensure a formal Non-Disclosure Agreement is signed with the Auditee and is in place prior to start of work.

ii. Regardless of the existence of a Non-Disclosure Agreement, the security auditing organization is ethically bound to maintain confidentiality and ensure non-disclosure of the auditee's information and security testing results.

iii. Auditing organizations must inform the auditee organisation, prior to the commencement of the audit assignment, about the requirement to share audit metadata and audit reports with CERT-In within five days of audit completion.

13.2.2 Planning the Audit Team and Tool Authorization

i. The information regarding audit team selected for conducting audit should be shared with the auditee and a documented approval regarding the same should be procured before the formal commencement of audit.

ii. The test plan shared by auditing organization must include both calendar time and man-hours.

iii. Ensure that a list of tools planned to be installed is provided to auditee organization along with a written confirmation that the

auditing organization is not violating any IPR or license norms while using and installing the tools.

iv. The auditing organization must have a thorough understanding of the tools they use, including their origin and functionality. These tools should be tested in a controlled test environment prior to deployment on the auditee's systems. The results of such testing must be formally reviewed and approved by an authorized representative of the auditee organization.

v. Appropriate written approvals must be obtained prior to conducting any penetration tests, and the installation of tools should be carried out in the presence of the auditee's system administrator.

13.2.3 Planning Audit Scope and Objectives

i. In order to ensure clarity about the deliverables, below mentioned points must be communicated clearly by the auditing organization to the auditee organization before the commencement of the Audit:

   a) Scope of audit shall clearly define the type of audit to be conducted i.e. VAPT (Vulnerability Assessment Penetration Testing), EAPT (External Attack Penetration Testing), DLA (Device Level Audit), Configuration Audit, Process Audit, Mobile Application Security Audit, Web Application Security Audit, API Security Audit, Compliance audit etc.

   b) Format of the Reports

   c) Standards or Frameworks to be used for conducting audit

   d) Assets covered in the scope

   e) Handling & retention of auditee data

   f) Timeline of the assessment phase

   g) Requirement to share audit metadata & reports with CERT-In

ii. Below mentioned points must be taken into consideration while finalizing the scope of Audit:
   a) Auditing organization may advise auditee organization to finalize the scope derived from centralized asset inventory to ensure that all the assets are covered in the scope.
   b) Auditing organization may advise auditee organization to explicitly mention the date up to which the scope / asset inventory has been updated and this date must be reflected in the audit reports.
   c) Version-specific details of web and mobile applications must be explicitly mentioned in the audit scope and report.

iii. Audit should not be performed just for the sake of compliance, but to secure the cyber infrastructure so as to protect the interest & goals of the auditee organization.

13.2.4 Planning Stakeholder Communication and Clarity

i. Ensure that there is no 'expectation gap' in the conduct of the audit. The 'expectation gap' refers to the difference between what the auditee perceives or expects from the audit and what the audit professionals understand the engagement to entail. This gap should be reduced or eliminated by clearly explaining, at the outset, the audit process, required artifacts, and expected deliverables.

ii. The auditing organization should provide clear communication to the auditee organization regarding any exemptions, limitations, and other constraints related to the audit.

13.2.5 Planning Report Handling and Distribution

A report distribution list comprising the official email IDs of designated auditee-side contacts should be obtained prior to report distribution. Additionally, the mobile number of the designated

contact should be collected for securely sharing passwords related to password-protected reports. Both the audit reports and their passwords must be shared exclusively with the authorized contact.

13.2.6 Planning for Risk Escalation and Issue Resolution

There should be a well-defined escalation matrix both for the auditee organization and auditing organization for addressing any problem encountered during the audit process which should be shared with respective authorities.

13.2.7 Planning Remote and High-Risk Test Scenarios

i. In case of remote testing, the identity of the auditor with mobile number and/or IP addresses must be disclosed and formal written permission must be obtained from the auditee organization, clearly outlining the tasks to be performed.

ii. Specific written permissions must be obtained from the auditee organization before conducting tests that involve survivability failures, denial-of-service (DoS), process testing, or social engineering.

iii. The auditing organization must notify the auditee organization in the event of any changes to the audit plan, change in the source test venue, identification of high-risk findings, or prior to conducting new, high-risk, or high-traffic tests. The auditee should also be informed if any testing issues arise. Additionally, the auditing organization should provide progress updates to the auditee at reasonable intervals.

14. Agreeing on the Terms of Engagement and Revisions to the Scope

14.1 Documentation of the Engagement Agreement

i. Before commencing a cyber security audit, it is essential to formally agree upon the terms of engagement between the auditing and auditee organisation. This agreement ensures clarity of purpose, establishes mutual expectations, and defines the responsibilities of all parties involved. A well-documented engagement agreement serves as the foundation for an effective and efficient audit process.

ii. The agreed-upon terms must be formally documented in an audit engagement letter. This document must be reviewed and signed by authorized representatives from both the auditing and the auditee organization. It serves as a binding reference point throughout the engagement.

14.2 Revisions to the Scope

It is recognized that, during the course of the audit, changes in circumstances or new findings may necessitate a revision to the originally agreed scope. In such cases:

a) Revisions must be proposed in writing, with justification for the change. Both parties must evaluate the impact of the revision on audit timelines, resource allocation, and deliverables.

b) Any changes must be approved by authorized representatives and documented as an addendum to the audit engagement letter or through formal amendment procedures.

c) The revised scope must be communicated to all relevant stakeholders to ensure alignment and continued cooperation.

14.3 Criteria for Revisions to the scope

i. Discovery of previously unidentified systems or processes that present significant risk.

ii. Changes in organizational structure, ownership, or regulatory environment.

iii. Security incidents or breaches occurring during the audit period.

15. Performance of the Audit

15.1 Guidelines for Auditee Organizations

15.1.1 Preparing the Audit Environment

i. To prevent a temporary increase in security measures solely for the duration of the audit, the auditee organization should limit notification about the auditing/testing to key personnel only. It is the auditee organization's discretion to identify who these key individuals are; however, they are generally expected to include personnel at the policy-making level, as well as managers responsible for security processes, incident response, and security operations.

ii. The auditee organization should refrain from implementing any unusual or major network changes during the auditing or testing period.

15.1.2 Managing Access and Testing Credentials

If privileged testing is necessary, the auditee organization must provide only temporary access such as login credentials, access tokens, certificates, or secure ID numbers and must ensure that all such privileges are revoked immediately upon completion of the audit.

15.1.3 Monitoring Audit Execution

i. The auditee organization must ensure that the tests agreed upon in the audit contract are being properly executed by the auditing organization, and that the prescribed timelines are adhered to, through the scheduled progress meetings.

ii. The auditee organization should actively track the closure of the assessment phase, re-validation phase, and overall audit completion.

15.1.4 Adhering to Regulatory Guidance

Auditee organization must implement the guidelines and advisories issued by CERT-In and/or Regulator from time to time in their auditing program.

15.2 Guidelines for Auditing Organizations

15.2.1 Pre-Audit Preparation and Compliance

i. A pre-audit discussion on the scope of work must be held between the auditing and auditee organizations to eliminate ambiguities, and ensure alignment with the applicable comprehensive standards and frameworks relevant to the domain and regulatory environment.

ii. The auditing organization must ensure that personnel with appropriate expertise and experience specific to the domain or type of audit are assigned to the engagement.

iii. The auditing organization must revalidate observations from the previous audit cycle, and any unresolved issues should be recorded as repeat observations in the current audit cycle.

iv. Organization must include the verification of compliance to CERT-In direction “Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet”

dated 28 April 2022 in every audit assignment and findings along with relevant evidences should be included in the audit report. Organizations may refer the method of verification document "Method of verifications to compliance with CERT-In Directions issued on 28.04.2022" available on CERT-In website at https://cert-in.org.in/PDF/Methods_of_Verification.pdf.

v. CERT-In updates, advisories and vulnerability notes should be incorporated in the audit practices.

vi. Auditing organizations must comply with all applicable regulations, acts and circulars issued by the government and regulators concerning data security & privacy.

vii. An official exchange of designated Points of Contact (PoCs) should be established between the auditing organization and the auditee organization. This ensures seamless coordination, clarity in communication, and regular interaction before, during, and after the audit process.

15.2.2 Conducting Secure and Ethical Testing

i. When dealing with high-risk vulnerabilities such as discovered breaches, a responsible and ethical approach. These vulnerabilities should be assessed and reported immediately to auditee organisation & CERT-In.

ii. Explicit written permission must be obtained from the auditee organization prior to conducting Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), or flood testing over the Internet to prevent disruption of services.

iii. Social engineering and process testing should be conducted in a controlled and ethical manner. When targeting general staff

(e.g., untrained or non-security personnel), such testing must utilize anonymized or statistical techniques—ensuring no individual is personally identified or penalized. The purpose is to evaluate overall awareness and the effectiveness of security processes, not to single out individuals.

Social engineering and process testing must only target group of employees explicitly included within the agreed audit scope. These tests must not involve external entities such as customers, business partners, vendors, or other third parties, unless specific written consent is obtained from the target organization. This ensures that all testing remains ethical and legally compliant.

iv. In critical environments where availability is a top priority, testing should be conducted in a passive manner to avoid any potential downtime or service disruption.

15.2.3 Managing Testing Environment and Approvals

i. The auditing organization must clearly specify the environment such as Test, Development, UAT, Pre-Production, or Production, in which the application has been tested during application security audit.

ii. The auditing organization is required to audit and test the website on the staging server or testing environment provided by the hosting service provider prior to issuing the Audit Certificate. Application hash values and version numbers must be obtained from the auditee and included in the audit report.

15.2.5 Ensuring Quality, Timelines, and Confidentiality

i. The auditing organization must ensure that all timelines and commitments made to the auditee organization are strictly adhered to.

ii. The security and confidentiality of auditee data must be effectively managed. Well-defined and documented procedures should be established for handling auditee data both during and after the audit.

iii. The auditing organization should implement the maker-checker concept to enhance the quality and effectiveness of security assessments. A separate verification team (checker) should be deployed to review and validate the work performed by the audit team (maker).

15.2.6 Incident Management and Escalation

The auditing organization should have an Incident Management Policy and related processes in place, including a clearly defined escalation matrix and procedures for addressing non-compliance. This incident response process should be shared with the auditee organization.

15.2.7 Review and Coordination

Regular meetings should be conducted between the auditing organization and designated representatives (SPOCs) of the auditee organization to review audit progress, with the objective of assessing and enhancing audit efficiency.

16. Forming an Opinion, Conclusion and Reporting

16.1 Drafting and Structuring the Report

i. Audit report format should be mutually agreed upon (Auditee organization and Auditing organization) and finalized before commencement of the audit.

ii. Audit report should be clear, precise and comprehensive to include all details of audit process, detailed scope, duration of audit, methodologies/standard used, tools, manual process, findings, prioritization, sampling decisions, manpower involved, exemptions, limitations and other constraints.

iii. All the assets provided in the scope by auditee organization must be mentioned in the report.

iv. Report versions – Draft / Final, etc. with date of issuance of each of them to be maintained and captured in the audit report.

v. Audit-related artifacts, such as hash values, versions, and timestamps, be captured by the auditee organization and shared with the auditing organization. These details should be prominently featured in the audit certificate and reports.

vi. The audit reports shall be signed only by the manpower declared to CERT-In, as listed in the organization's snapshot information available on the CERT-In website. The report must be signed by the Auditors who conducted the audit. It should then be reviewed and signed by a designated Reviewer who is not part of audit team and is from mid-management, to ensure an unbiased and quality review. Finally, the report must be authorized and signed by the Head of the Auditing Organization (e.g., Director, Partner, or CEO), certifying the completeness, accuracy, and integrity of the audit findings and

recommendations. The audit certificate must be signed by both the Lead Auditor and the Head of the Auditing Organization.

16.2 Executive Summary and Risk Categorization

i. The audit report should include an executive summary providing a concise overview of the audit findings, including associated risks to the organization and the overall security posture of the audited application or infrastructure. This summary is intended for the board members or top management of the auditee organization. The executive summary should translate the technical findings into relevant business risks and the overall security posture of the audited application or infrastructure.

ii. Auditors are required to implement both CVSS and Exploit Prediction Scoring System (EPSS) frameworks within their audit reports. The observations/vulnerabilities in the report must be categorized based on the Common Vulnerability Scoring System (CVSS) for severity and supplemented with the Exploit Prediction Scoring System (EPSS) to assess the likelihood of real-world exploitation. Every reported observation / vulnerability shall be mapped with Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) number.

16.3 Practicality of Remediation and Follow-up Actions

i. Ensure that suggested controls and remedies are practical and implementable.

ii. Vulnerabilities classified as ‘critical’/‘high’ in the severity score are required to be notified by the auditor to the auditee organization during the course of audit on as and when found basis. The same is also to be reported in the Final Outcome Report.

iii. Audit report should mention appropriate timelines for closure of vulnerabilities according to severity.
iv. After remediation actions, follow-up audits should be performed by auditing organizations to verify closure of vulnerabilities and non-conformities highlighted in the previous audit.
v. The Final audit report should be issued after the closure of vulnerabilities & completion of follow-up audit of the application hosted on production environment. If the audit scope is limited to the staging platform, the report must explicitly state that the audit was not conducted on production environment.

16.4 Reporting of High Risk Vulnerabilities

High-risk vulnerabilities such as discovered breaches, vulnerabilities with known high exploitation rates, unmonitored, or untraceable access, or those that may pose an immediate risk to life, must be reported to the auditee immediately upon discovery, along with a recommendation for a practical solution.

16.5 Report Delivery and Secure Communication

i. The auditing organization should use only official email IDs for sharing audit reports and related data with the auditee organization.
ii. The audit outcome & related matters should only be communicated to the specified Point of Contact (PoC) of the auditee organization. The audit outcome should only be shared using secure methods such as use of passwords, encryption etc.
iii. All communication channels for delivery of report are end to end confidential.

16.6 Data Handling and Disclosure Guidelines

i. The sharing and disclosure of auditee-related data should be done with the prior consent of the auditee organization. However, disclosures mandated by law or required by designated regulatory bodies or competent authorities in India (such as CERT-In) may be made by the auditing organization without additional consent. The auditee/project-related data shall not be shared with or disclosed to any overseas entity or partner, unless specifically authorized in writing by the auditee organization.

ii. In case of the incidents where client audit related data is leaked to unauthorized entity (intentionally or unintentionally), the auditing organization should inform the auditee about the incident and take all necessary actions to address the incident as may be required.

17. Communication with those Charged with IT Governance

i. The auditing organization will need clear and unambiguous direction from auditee management (written rules of engagement), clearly defined scope for security audit and input on what is required for planning & assessment, requirement analysis, test execution & analysis, results and documentation.

ii. The audit report should be presented to the top management of the auditee organization by the auditing organization.

iii. Entry and Exit conferences should be organized and attended by the senior management of the auditee organization to ensure alignment and commitment throughout the audit process.

The entry conference is crucial for setting clear expectations and ensuring a smooth initiation of the audit. During this meeting, the audit's scope, objectives, timeline, and key responsibilities should be thoroughly discussed and agreed upon, ensuring both parties are aligned on the process. A formal presentation should be delivered to the organization's Board and senior management during onboarding, clearly outlining the auditor's understanding of the scope, the audit methodology to be adopted, key phases of the engagement, and expected timelines. This helps establish transparency, builds confidence, and ensures that the audit begins with mutual understanding and buy-in at the highest levels.

The exit conference serves as a structured forum for the auditing organization to present preliminary findings, highlight key risks, vulnerabilities, and areas of concern identified during the audit. A detailed presentation should be made covering audit observations, the organization's overall security posture, and associated risks, to

enable informed decision-making. Recommendations for remediation should be reviewed, and the auditee's questions or concerns must be addressed to ensure full understanding. The exit conference also provides an opportunity to outline the next steps, including agreed-upon remediation actions and timelines for resolution. This ensures that the audit concludes formally with a clear and actionable roadmap for addressing the identified issues.

iv. The auditing organization should maintain regular contact with the auditee organization even after the audit assignment is completed, as part of a professional relationship. A communication channel should be established to inform or alert the auditee about the latest developments in cyber security that are relevant to their environment.

18. Audit Evidence and Documentation

i. Auditee organizations must seek the working notes upon completion of the audit (provisions for the same should be included in the audit contract) and should ask for audit evidence collected during the assessment be submitted as an appendix along with the final audit report.

ii. In system or compliance audits, artifacts and evidence demonstrating both compliance and non-compliance with controls should be captured and documented by the auditing organization in the audit report.

iii. All the observations made during the audit are well supported with objective evidences and all evidences are compiled carefully and correctly with the report. All the evidence gathered during the process of audit is presented in a manner that the decision makers are able to use them effectively in making credible risk-based decisions.

iv. Audit evidence must be stored securely, with access restricted to authorized personnel only. Proper measures (encryption, access controls, etc.) must be implemented to ensure confidentiality, integrity, and availability of the evidence throughout the audit lifecycle.

v. The auditee organization may request clarifications or justifications for any evidence presented, and the auditing organization must respond within a mutually agreed timeframe.

vi. In case, the scope is related to digital forensic investigation, then, in case such forensic investigation faces constraints due to unavailability/ inadequacy of evidence/ logs then the audit report should explicitly bring out the same and recommend log details to be captured. The report may also encompass a confirmation status to verify the resolution of immediate issues identified in the Root Cause Analysis

(RCA), ensuring that the necessary fixes have been implemented. Additionally, it should detail the completion of cleanup procedures to eliminate any foothold or access points established by threat actors within the infrastructure.

19. Consequences of Non-Compliance to Guidelines and Terms and Conditions of Empanelment

CERT-In has developed and issued a framework to improve quality of audits comprising enabling actions as well as deter & punish mechanism. The framework is available on CERT-In website at https://cert-in.org.in/PDF/RoD_Interaction_session_website.pdf. Following graded actions will be taken by CERT-In and auditee organization in case of adverse reports, violation of these guidelines & terms and conditions of empanelment and poor quality of audits:

a) Move to watch list with warning & written commitment
b) Suspension
c) Debarment as per GFR and De-empanel by CERT-In
d) Penal & Legal Actions

Deter & Punishment matrix –

S.No	Grade: Severity (Moderate to High)	Indicative parameters for Actions	Actions
1.	Move to watch list with warning & written commitment	1. Inadequate closure of Non Compliances (NCs). 2. Lack of relation between Noting & issues raised. 3. Inadequacy of sample details, issues covered, improper conclusions. 4. Violating CERT-In Terms & Conditions (having minor	CERT-In to issue show cause and obtain corrective action report from Auditing Organisations with issue warning along with written commitment.

S.No	Grade: Severity (Moderate to High)	Indicative parameters for Actions	Actions
		impact), First adverse report includes missing of maximum 2 vulnerabilities, conflict with auditee, first instance of noncompliance to CERT-In data collection framework, etc	
2.	Suspension	1. Adverse feedback from Auditee regarding technical competency auditor's attributes etc. 2. Repeated failure in respect of audit planning, coverage of audit, Highlighted in CERT-In analysis & observations etc. 3. Issues appearing soon after conduct of audit. 4. Violating CERT-In Terms & Conditions (having major impact), multiple adverse report of missing vulnerabilities, multiple instance of non-compliance to CERT-In data collection framework, etc.	Suspension to be revoked based on satisfactory submission of Corrective Actions and witnessing, if needed

S.No	Grade: Severity (Moderate to High)	Indicative parameters for Actions	Actions
3.	Withdrawal of Empanelment	Auditing malpractices, Substandard services, failure to cover scope of work, etc.	Actions as per GFR and O.M No. F.1/20/2018-PPD dated 2nd November 2021 of Department of Expenditure.
4.	Penal & Legal Actions	Breach of Trust, Digital break-in, Damage & Attempt to damage auditee interests & infrastructure, etc.	As per applicable penal & legal acts / laws

20. Conclusion and Feedback mechanism

i. The objective of these guidelines is to provide a structured, standardized, and practical framework for conducting cyber security audits across organizations. By outlining uniform standards, clearly defining roles and responsibilities, and promoting continual improvement, these guidelines aim to strengthen the overall cyber resilience of the ecosystem. It is expected that these guidelines will serve as a reference for both CERT-In empaneled auditing organizations and auditee entities, ensuring that audits are carried out consistently, effectively, and securely. The document is intended to support the audit process from planning to reporting, ultimately contributing to the broader goal of safeguarding the nation's cyber infrastructure.

ii. CERT-In encourages a collaborative and iterative approach to strengthening the cyber security audit ecosystem. Both auditing organizations and auditee organizations are invited to share their experiences, provide constructive feedback on the audits conducted, highlight any challenges encountered during the audit process, and suggest improvements to these guidelines. Such inputs are vital to ensuring that the audit framework remains practical, relevant, and aligned with evolving technological and threat landscapes. Organizations are requested to submit their feedback or suggestions to empanelment@cert-in.org.in.