

Analysis of Cyber Security Audit Policy Guidelines issued by CERT-In

Issued by- Indian Computer Emergency Response Team (CERT-In)-Ministry of Electronics and Information TechnologyGovernment of India

Incorporated on 28th February,1981

43 years of Reliable, Responsive and Responsible Client Services

CUSTOMISED DELIVERY | OBJECTIVE ADVICE KNOWLEDGE INSIGHT | CLEAR FORESIGHT

JHS

The Strategic Imperative

The CERT-In guidelines represent a fundamental shift from compliance-based auditing to strategic risk management. Organizations that embrace this change proactively will build stronger cyber resilience and gain competitive advantage, while those that resist face legal, operational, and security risks.

Critical Message: This is not just about changing audit vendors or adding checklist items - it's about transforming how organizations think about, manage, and invest in cybersecurity as a strategic business capability.



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. Regular cyber security audits and assessments can improve an organization's security posture, detect vulnerabilities, and ensure regulatory compliance.`

These guidelines serve two purposes:

- ✓ **Assist auditee organizations in preparing for audits, understanding requirements, and addressing deficiencies**
- ✓ **Provide auditing organizations with a structured framework to conduct rigorous, fair, and transparent cyber security audits**

The circular explicitly states:

"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."



Authority for Issuance of Guidelines

Legal Foundation

Sub-section (1) of section 70B of the Information Technology (IT) Act, 2000 (21 of 2000) provides that the Central Government shall appoint the Indian Computer Emergency Response Team (CERT-In) as the agency for the purposes of the Act.

CERT-In Functions

Sub-section (4) of section 70B provides that CERT-In shall perform prescribed functions in cyber security, including "issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents."

Binding Authority

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

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.



Establish Uniform Standards

Ensure that all cyber security audits follow a common set of standards and procedures, promoting consistency in audit quality, evaluation criteria, and reporting.



Provide Clarity

Define the roles, responsibilities, and expectations for both auditing organizations and auditee organizations, ensuring mutual understanding of the audit process and deliverables.



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.

Applicability

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



CERT-In empaneled Auditing Organizations

Organizations empaneled by CERT-In to undertake audits, including vulnerability assessments and penetration testing of computer systems, networks and applications of various organizations.

Auditee Organizations

Organizations that own or operate the systems, processes, and infrastructure being evaluated by the CERT-In empaneled auditing organizations, in both public and private sectors.

Definitions

Key terms used throughout this document are defined as follows:

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.

Audit Evidence

Information, documentation, logs, observations, or other forms of data collected during the audit that substantiate findings and support conclusions.

Non-Conformity

A condition wherein a process, control, or practice fails to meet the prescribed standards, regulatory requirements, or internal policies.

Vulnerability Assessment

Examination of an information system to determine the adequacy of security measures, identify deficiencies, and confirm the adequacy of measures after implementation.

Penetration Testing

A security testing methodology in which components are actively tested to identify and exploit potential vulnerabilities to determine if they can be compromised.

Vulnerability Classification

Categorization using CVSS (Common Vulnerability Scoring System) for severity and EPSS (Exploit Prediction Scoring System) for likelihood of exploitation.

Scope of Engagements Covered

The types of cyber security audits and assessments that fall within the scope of this document include, but are not limited to:
The circular defines extensive 26+ audit categories beyond traditional VAPT



Compliance Audits

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



Risk Assessments

The process of identifying and evaluating risks arising from cyber threats, vulnerabilities, and potential cyberattacks that could impact organizational operations.



Network Infrastructure Audits

Comprehensive review of network components, including hardware devices, software, configurations, and security measures.



Application Security Testing

Assessing web applications, mobile applications, and APIs to identify security vulnerabilities in architecture, components, and configuration.



Cloud Security Testing

Evaluating the security measures, configurations, and vulnerabilities of cloud-based systems, applications, and infrastructures.



Emerging Technology Audits

Evaluation of AI systems, blockchain, IoT/IIoT devices, and other emerging technologies for security, ethical alignment, and resilience.

360-Degree Coverage: "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."

Basic Principles in Audit

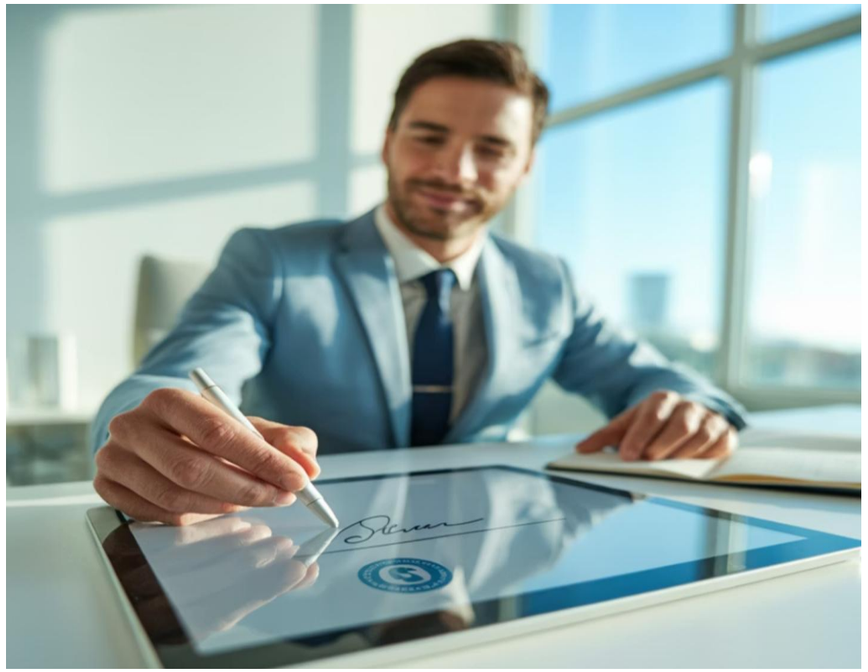
The effectiveness of a cyber security audit relies on adherence to fundamental principles that guide the auditor's conduct:

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.

Top Management Responsibility

“

The complete audit process of the information infrastructure must be undertaken up by the auditee organization itself... This responsibility must not be delegated."



Applicable Standards and Frameworks



Auditing organizations must utilize industry standard methodologies and best practices for security testing:

- Solely tools-based testing should be discouraged as it may overlook non-automated components
- Audits should include discovery of all known vulnerabilities based on comprehensive standards/frameworks like ISO/IEC, OWASP, and CSA Cloud Controls Matrix
- 'Cyber Security Audit Baseline Requirements' document published on CERT-In's Website should be used to build audit programs
- Guidelines and directions issued by CERT-In and regulators must be included in audit scope by default
- Applications developed without secure design and development practices should not be considered for assessment

Auditee Responsibility

Governance and Oversight

Top management should review & approve the audit program, scope and remedial measures. The responsibility for maintaining a robust cyber security posture ultimately rests with the auditee organization, not the auditor.

Risk Acceptance

Risk treatment techniques for any reported vulnerabilities must be authorized & accepted by the head of the auditee organization. Any exceptions must be authorized by the head of the organization.

Remediation and Follow-up

After receiving audit findings, the auditee is responsible for implementing the recommended actions. Vulnerabilities should be patched by owners/developers at the earliest.

Internal Monitoring

Continuous internal audits/assessments should be carried out by auditee entities. 'Secure by Design' principles must be included as mandatory requirements in RFPs for application development.

Auditor Responsibility

Role and Accountability

Auditors evaluate the effectiveness of security measures, verify compliance, and provide recommendations for improvement. Their responsibility is limited to reviewing and reporting on the state of security at the point in time of the audit.

Personnel Conduct

Audit team members must adhere to practices that ensure confidentiality, security, and privacy of information. All must have valid NDAs and demonstrate high standards of ethical practices and professional conduct.

Data Handling

Audit-related data must be treated as confidential, stored only on systems located in India with adequate safeguards, and wiped from auditor's laptops after project completion.

Awareness and Training

Auditing organizations should arrange in-person sessions for clients on audit awareness, covering fundamentals of cyber security audits and CERT-In initiatives.

CERT-In Affiliation

Auditing organizations shall not use the CERT-In logo or make reference to their association with CERT-In without prior written permission. They may use the words "This Organization is empaneled by CERT-In for providing Information Security Auditing Service."





Quality Control of Auditing Organizations

CERT-In Oversight

CERT-In at any point in time can be a part of the audit team to assess the quality and maturity of audit. CERT-In reserves the right to seek/audit information from auditing organizations for any project done within the empanelment period.

Feedback Mechanism

Auditee organizations must provide feedback on the audit conducted to CERT-In as well as to the auditing organization. Feedback/complaints to CERT-In would help improve the quality of selecting auditing organizations in future.

Consequences of Poor Performance

In case of adverse feedback or lapses in audit assignments, actions as per the Deter and Punish Framework published by CERT-In may be taken without any reminder or notice.

Technical Standards Revolution

Dual Scoring System Implementation

CVSS (Common Vulnerability Scoring System)

For severity assessment of all identified vulnerabilities

EPSS (Exploit Prediction Scoring System)

For likelihood of exploitation in the wild

Mapping Requirements:

- Every vulnerability must be mapped to **CWE (Common Weakness Enumeration)**
- Cross-reference with **CVE (Common Vulnerabilities and Exposures)** where applicable
- Evidence-based prioritization for remediation

Prohibited Approaches:

- **No Tool-Only Audits:** *"Solely tools-based testing should be discouraged"*
- **No Limited Checklists:** OWASP Top 10, SANS Top 25 alone are insufficient
- **Manual Validation Required:** All automated findings must be manually verified

Selection of Auditor

Utilizing Snapshot Information

The snapshot information of skills and competence of CERT-In empaneled auditing organizations should be utilized to identify and select auditing organizations by mapping requirements with competence.

Information available on the CERT-In website can help with:

- Evaluation of manpower and skillset details
- Experience relevant to information security audits
- Categories of audits conducted
- Sector-wise audits carried out in last 12 months
- Technical manpower deployed for audits
- Tools used in various audits

Selection Process

Auditee organizations should:

- Interview and select resources aligned by auditing organizations for competency and experience
- Verify technical credentials of manpower deployed
- Verify identity, official documents, and designations of the auditing team
- Check domain of audit conducted, previous audits, and other relevant details

Contractual Guidelines

Contracts for critical applications should be awarded for 2-3 years to enable continuous audits at a defined frequency. Contractual agreements should allow the auditee to stop the audit and choose another auditing organization if necessary.

Planning the Audit

1

Define and Finalize Audit Scope

The scope should include the entire cyber infrastructure: systems, applications, network, OT/ICS environment, cloud architecture, APIs, databases, and hosting infrastructure. The scope must be derived from the consolidated asset inventory and vetted by the internal audit team.

2

Determine Audit Frequency

Cyber security audits should be conducted at least once a year. Additional audits should be performed after every major change in infrastructure and application, based on criticality.

3

Identify Critical Assets

Critical databases/applications must be identified and included in the scope. For critical databases, audits should include configuration audit. For critical applications, audits should include DAST and SAST.

4

Plan Team and Stakeholder Coordination

A technical team should be assigned as point of contact for assisting and monitoring the auditing organization. Regular interaction between the technical team and auditors should be scheduled.

Critical Timeline Requirements

Immediate Action Items (Organizations Must Act Now):

1 Within 5 Days of Audit Completion

- Auditors must submit metadata to CERT-In
- High-risk vulnerabilities must be immediately escalated

2 Annual Mandate

- **Minimum Annual Audits:** All ICT systems must be audited at least once yearly
- **Major Change Triggers:** Audit required after significant infrastructure changes
- **Continuous Assessment:** Periodic audits based on asset criticality

3 Follow-up Requirements

- **Mandatory Follow-up Audits:** Must be included in scope/RFP
- **Remediation Verification:** Required after vulnerability closure
- **Closure Certification:** Comprehensive report confirming issue resolution



Critical Prohibitions & Conflict Management

Independence Requirements:

No Implementation + Audit

Same entity cannot implement controls and audit them

No Outcome-Based Payments

Audit fees cannot be contingent on results

No Remediation by Auditors

Clear separation of audit and remediation activities

Data Protection Mandates:

India-Only Storage

Audit data must be stored only in India

Secure Disposal

Forensic-grade data deletion required post-audit

Access Control

Strict restrictions on temporary staff access

Disposal Certification

Written confirmation of data destruction required



Agreeing on Terms of Engagement

Documentation Requirements

Before commencing a cyber security audit, the terms of engagement between the auditing and auditee organization must be formally agreed upon and documented in an audit engagement letter, signed by authorized representatives from both organizations.

Revisions to Scope

During the audit, changes in circumstances or new findings may necessitate a revision to the originally agreed scope. Revisions must be:

- Proposed in writing with justification
- Approved by authorized representatives
- Documented as an addendum
- Communicated to all relevant stakeholders

Performance of the Audit

Pre-Audit Preparation

A pre-audit discussion on the scope must be held to eliminate ambiguities. Personnel with appropriate expertise must be assigned to the engagement. Previous audit observations must be revalidated.

Secure Testing

High-risk vulnerabilities must be reported immediately. Written permission must be obtained before conducting DoS/DDoS testing. Social engineering must be conducted ethically, targeting only groups explicitly included in the scope.

Testing Environment

The environment (Test, Development, UAT, Pre-Production, or Production) must be clearly specified. Application hash values and version numbers must be obtained and included in the audit report.

Quality Assurance

Timelines and commitments must be strictly adhered to. The maker-checker concept should be implemented to enhance quality, with a separate verification team reviewing the audit team's work.



Forming an Opinion and Reporting

Report Structure and Content

Audit reports should be:

- Clear, precise, and comprehensive
- Include details of audit process, scope, methodologies, tools, findings, and limitations
- Mention all assets provided in the scope
- Include audit-related artifacts (hash values, versions, timestamps)
- Signed by auditors who conducted the audit, a reviewer, and the Head of the Auditing Organization

Risk Categorization

Reports must implement both CVSS and EPSS frameworks. Observations must be categorized based on severity and likelihood of exploitation. Every vulnerability should be mapped with CWE and CVE numbers.

Secure Delivery

Reports should be shared using only official email IDs and secure methods such as passwords and encryption. Communication should be limited to specified Points of Contact.

Communication with IT Governance

Entry Conference

A formal presentation should be delivered to the organization's Board and senior management during onboarding, clearly outlining the audit's scope, methodology, key phases, and expected timelines. This establishes transparency and ensures mutual understanding.

Regular Updates

Throughout the audit process, regular meetings should be conducted between the auditing organization and designated representatives of the auditee organization to review progress and enhance audit efficiency.

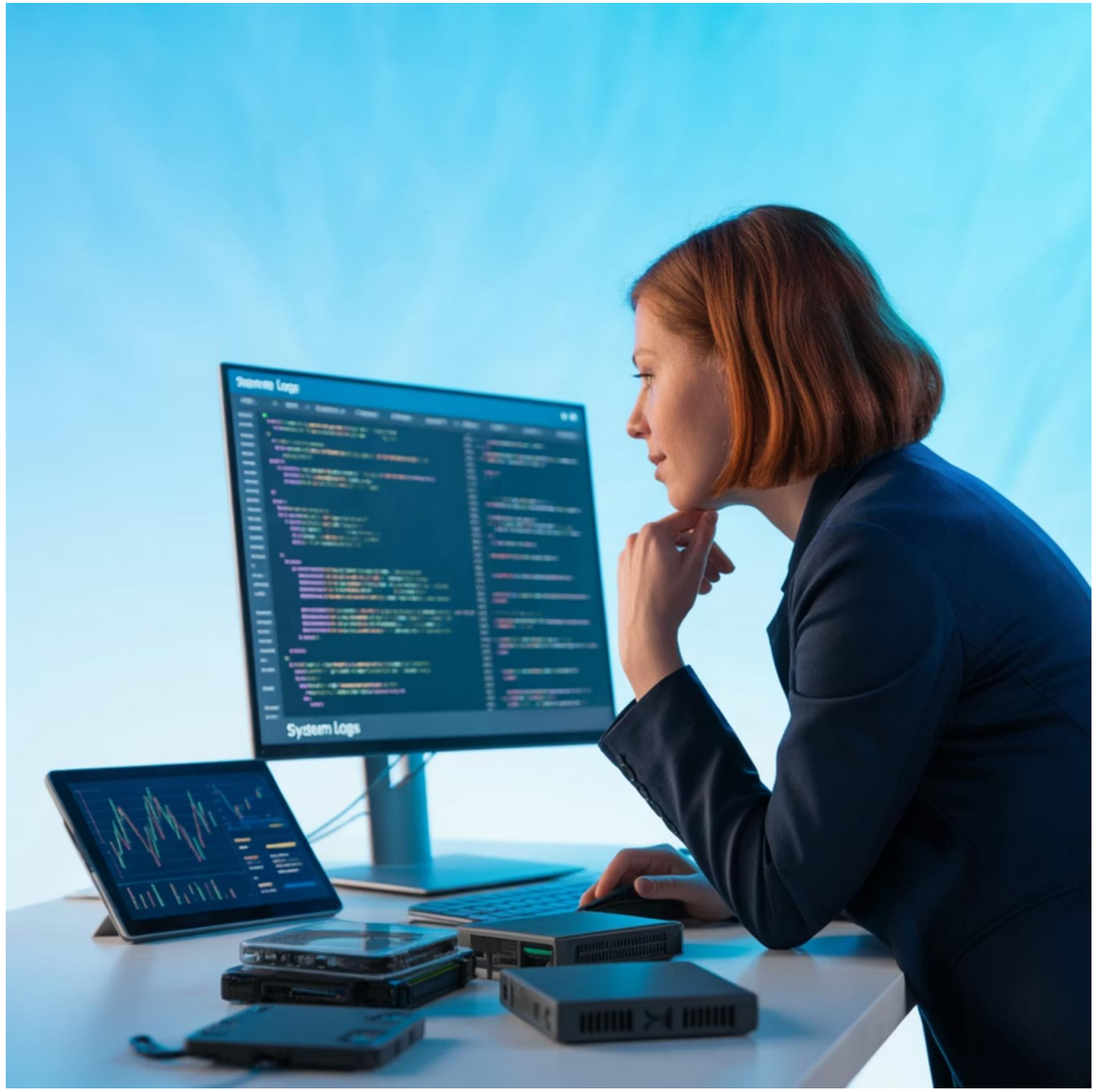
Exit Conference

A detailed presentation covering audit observations, the organization's overall security posture, and associated risks should be made to enable informed decision-making. Recommendations for remediation should be reviewed, and next steps outlined.

Ongoing Communication

The auditing organization should maintain regular contact with the auditee organization even after the audit is completed, establishing a channel to inform or alert the auditee about relevant developments in cyber security.

Audit Evidence and Documentation



Proper handling of audit evidence is crucial for the integrity and effectiveness of the audit process:

Evidence Collection

All observations must be supported with objective evidence. Artifacts demonstrating both compliance and non-compliance should be captured and documented in the audit report.

Secure Storage

Audit evidence must be stored securely, with access restricted to authorized personnel only. Proper measures (encryption, access controls) must be implemented to ensure confidentiality, integrity, and availability.

Working Notes

Auditee organizations should request working notes upon completion of the audit. Provisions for this should be included in the audit contract.

Application Development Prerequisites

The circular states: ***"Applications developed without any secure design and development practices should not be considered for assessment and audits."***

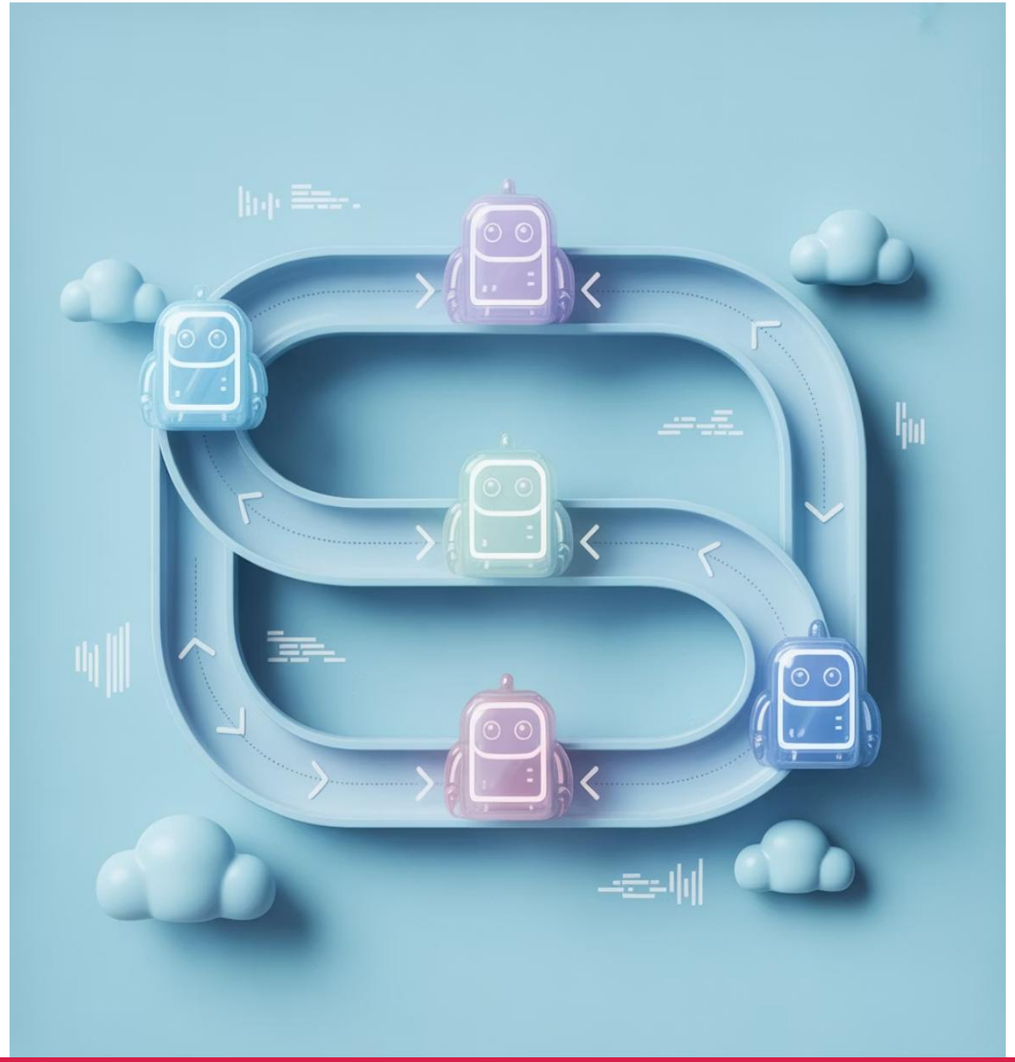
Pre-Audit Requirements:

Secure Design Confirmation
Applications must be designed with secure practices

SAST Requirement
Software developers must perform Static Application Security Testing

RFP Integration
Secure development must be mandatory in tenders

Verification Documentation
Evidence of secure development practices required



Hash Values and Version Control:

- **Audit Artifacts Mandatory:** Hash values, versions, timestamps must be captured
- **Version Control:** Assets in audit scope must be backtrackable
- **Change Management:** Formal processes required for all changes

Critical Success Dependencies

What Organizations Cannot Afford to Ignore:

Legal Mandate

Non-compliance carries legal consequences under IT Act 2000

Comprehensive Scope

Traditional VAPT alone is no longer sufficient

Quality Standards

Tool-only audits and limited checklists are explicitly prohibited

Management Accountability

Security ownership cannot be delegated

Continuous Nature

One-time compliance is not sufficient; ongoing commitment required

Investment Requirements:

People

Skilled internal teams for audit coordination and remediation

Process

Robust change management, asset inventory, and risk management

Technology

Comprehensive security controls, monitoring, and response capabilities

Partnership

Long-term relationships with qualified CERT-In empaneled auditors

Strategic Implementation Roadmap

Phase 1: Immediate Compliance (0-90 days)

1. Auditor Verification: Confirm current auditors are CERT-In empaneled
2. Scope Assessment: Review current audit scope against 26+ categories
3. Gap Analysis: Identify missing audit types and coverage areas
4. Management Engagement: Secure top management commitment and oversight
5. Update RFPs and contracts with CERT-In compliance requirements

1

Phase 2: Process Enhancement (3-6 months)

2

1. Infrastructure Hardening: Implement MFA, patch management, asset inventory
2. Policy Updates: Align with secure development and vendor management requirements
3. Team Training: Ensure internal teams understand new requirements
4. Contract Updates: Revise auditor agreements for compliance

Phase 3: Culture Transformation (6-12 months)

3

1. Strategic Integration: Align audits with business risk management
2. Continuous Monitoring: Implement ongoing assessment capabilities
3. Vendor Integration: Extend requirements to third-party relationships
4. Innovation Adoption: Prepare for AI, blockchain, and emerging technology audits
5. Implement dual scoring (CVSS/EPSS) and mapping (CWE/CVE)

Disclaimer

For the intended recipients only | Privileged & Confidential

- This presentation contains writers' interpretation of CERT-In guidelines and should not be considered as legal advice or official regulatory guidance
- Organizations should consult qualified legal counsel and directly reference official CERT-In publications for compliance requirements
- We do not warrant that compliance with these interpretations will ensure full regulatory compliance
- Information is based on CERT-In guidelines available as of the date of this presentation and is subject to regulatory updates and amendments
- We have exercised reasonable care in preparing this analysis but makes no warranties regarding completeness, accuracy, or reliability
- Organizations should verify current regulatory requirements directly with CERT-In before making compliance decisions
- This presentation is for informational purposes only and does not constitute a formal audit, assessment, or certification
- Any specific compliance requirements for your organization may vary based on sector, size, and operational context
- Implementation recommendations require customized assessment based on individual organizational circumstances
- We accepts no responsibility for decisions made based solely on this presentation
- Organizations assume full responsibility for their compliance strategies and implementation decisions
- Our liability is limited to the scope of formally engaged professional services under executed agreements