ERGO

KHAITAN &CO ADVOCATES SINCE 1911

# CERT-In's comprehensive Cyber Security Audit Policy guidelines:

## A bold step towards global best practices and elevating cyber security audits in India

1 August 2025

On 25 July 2025, the Indian Computer Emergency Response Team (CERT-In) constituted under the Information Technology Act 2000 (IT Act) issued the 'Comprehensive Cyber Security Audit Policy Guidelines' (Audit Guidelines). The Audit Guidelines are applicable to:

(i) CERT-In empanelled auditing organisations:
Information security auditing organisations empanelled with the CERT-In to perform cyber security audits of auditee organisations (Auditors).

(ii) Auditee organisations:
Entities (public or private) whose information and communication infrastructure are subject to audit by the Auditors (Auditees). For instance, Auditees would include private companies, banks, fintech platforms, etc.

The Audit Guidelines, issued pursuant to CERT-In's statutory mandate, are binding on Auditors and Auditees. They aim to standardise cyber security audit practices, clarify roles and responsibilities, and support remediation and continuous improvement. Failure to provide any information as requested by the CERT-In or non-compliance of any directions issued pursuant to the Audit Guidelines may be punishable with a monetary fine which could extend to INR 1,00,00,000 (Indian Rupees One Crore) (approx. USD 115,000) or an imprisonment for a term which could extend to 1 (one) year or with both.

## The Audit Guidelines cover the following key aspects:

1. **Scope of audit engagements**: The Audit Guidelines outline various types of cyber security audits, such as compliance audits, vulnerability assessments, source code review, application security testing, artificial intelligence system audits, digital forensic readiness assessment, internet of things (IoT), etc, while clarifying that the list is not exhaustive and additional assessments may be carried out as necessary. Audits are to cover the full cyber infrastructure of the Auditees, including critical systems, applications, cloud, databases, code, data security, and incident response, third-party/vendor risks and follow-up audits to verify remediation.

2. **Audit standards**: Cyber security audits are to avoid over-reliance on automated, tools-based testing which can miss critical manual or non-automated elements. Audits should draw from comprehensive frameworks such as ISO/IEC standards, CSA Cloud Controls Matrix, OSSTMM, and various OWASP guides, along with applicable regulatory requirements and CERT-In directions. Applications lacking secure design and development practices are to be excluded from the audit scope, with written notice of such exclusion provided to the Auditee and a copy marked to CERT-In.

3. **Frequency of audits:** At least 1 (one) audit annually is mandatory, with additional audits optional for the Auditee. However, major changes, such as system overhauls, technology migrations, or configuration updates impacting sensitive data or critical infrastructure will be subject to a cyber security audit prior to implementation. Sectoral regulators may decide to increase the audit frequency based on the organisational size, asset criticality and complexity of digital infrastructure, etc.

4. **Hosted and third-party infrastructure:** If a website or service is hosted on a third-party owned web server, the responsibility for auditing such server, its operating system, hosting software, and backend

applications lies with such third party. However, the organisation owning the website content, that is hosted on such third-party web server, remains responsible for ensuring that its data and software components are audited by a CERT-In empanelled auditor.

5. **Execution of agreements**: Auditees should enter into detailed audit contracts/agreements with the Auditors, which should, *inter alia*, set out the audit criteria, plan, tasks, timelines, reporting and data-handling requirements, follow-up audit clauses, NDAs, and an escalation matrix.

6. **Auditees' key responsibilities**:

| | |
|---|---|
| Selection of auditors | Auditees and sectoral regulators may refer to the snapshot information available regarding Auditors on CERT-In's website to identify and select empanelled Auditors whose competencies and domain expertise align with their audit requirements. |
| Approval of top management / board | Top management are required to review and approve the audit programme, scope, and remediation measures in a time-bound manner, and authorise the risk treatment plans for reported vulnerabilities, including any exceptions. |
| Disclosure in annual reports | The frequency and broad scope of audits are to be included in the annual reports. |
| Post-audit integrity | Post-audit, no changes to application or infrastructure code are permitted after the audit certificate is issued. The Auditees are required to share audit artifacts (e.g., hash values, version numbers, timestamps) with the Auditors for inclusion in the audit report. Robust version control and change management are to be implemented to ensure full traceability of audited assets. |

7. **Auditors' key responsibilities**:

| | |
|---|---|
| Independent conduct of Auditors | Auditors should remain free from bias, conflicts of interest, and external influence. Payments to Auditors should not be linked to the outcome of the audit. Audit fees should instead be based on predefined scope, deliverables, and timelines. If Auditors encounters any coercion, pressure tactics, or attempts by the Auditees to influence the audit, the matter should be promptly reported to CERT-In. |
| Handling audit related data | (i) Auditee-related data should be stored only on systems located within India. During the audit engagement, all audit-related data should be stored in encrypted form on the Auditor's laptop. Upon audit completion, this data is required to be permanently and irreversibly deleted. A formal certificate to this effect should be issued to the Auditee.<br>(ii) Auditee-related data may be retained only for the duration specified in the engagement agreement between the Auditor and the Auditee or applicable regulatory guidelines. In the absence of such specification, data may be retained for a maximum of 1 (one) year from the audit's completion.<br>(iii) The audit reports shall be signed by the Auditors who conducted the audit and are listed in the Auditor organisation's snapshot information submitted to CERT-In. The audit report will subsequently be reviewed and signed by a designated reviewer, who is not part of the audit team and holds a mid-management role. Finally, the report should be authorised and signed by the head of the Auditor organisation (e.g., Director, Partner, or CEO), certifying the accuracy, completeness, and integrity of the audit findings and recommendations. |
| Responsible approach of Auditors | For high-risk vulnerabilities, including discovered breaches, Auditors are required to assess and report them immediately to both the Auditee and CERT-In. Additionally, Auditors are to conduct audits and testing on the staging or testing environment provided by the hosting service provider before issuing the audit certificate. |

8. **Classification of vulnerabilities**: All vulnerabilities identified during cyber security audits are to be classified using two key frameworks: (i) CVSS (Common Vulnerability Scoring System) to assign a numerical score based on severity; and (ii) EPSS (Exploit Prediction Scoring System) to estimate likelihood of a vulnerability being exploited in real-world scenarios.

9. **CERT-In's oversight in audits**: CERT-In may participate in the audit activities conducted by the Auditors to assess the quality of the audit process. The Auditors are to clearly inform the Auditees in writing if CERT-In is participating in any phase of their audit. Additionally, CERT-In reserves the right to seek information or conduct its own review of any audit engagement carried out by the Auditors during the empanelment period. Further, Auditors are required to submit audit information to CERT-In in the prescribed format within 5 (five) days of completing an audit.

10. **Consequences of Auditors' failure to comply with Audit Guidelines and poor quality audits**: Any adverse feedback or identification of lapses, non-compliance, or deficiencies in the audit process of the Auditors are to be reported to CERT-In by the Auditees. Based on the severity of the issues, CERT-In may take graded enforcement actions against the Auditors, including issuance of warnings with placement on a watch list, seeking written commitments for corrective action, temporary suspension, debarment from future assignments, de-empanelment, and/or initiation of legal or penal proceedings.

## Comments

The Audit Guidelines significantly tighten India's cyber security audit regime. Mandatory annual audits, stringent planning and reporting requirements, and granular oversight by CERT-In mean that Auditees will need to relook at and strengthen how they approach cyber security compliance in a holistic manner. This will require early engagement with CERT-In empanelled Auditors, stronger internal governance, and legal teams revisiting all audit contracts and requests for proposal (RFPs) to ensure alignment with the new standards. Auditors will also need to align with the new framework by following prescribed methodologies, delivering evidence-backed reports, sharing audit information with CERT-In within prescribed timelines, and ensuring strong confidentiality and incident management practices. These measures allow an environment based on transparency and accountability to prosper, which is designed to benefit all stakeholders involved.

- *Supratim Chakraborty (Partner); Harsh Walia (Partner); Shobhit Chandra (Counsel); Shramana Dwibedi (Senior Associate) and Himeli Chatterjee (Associate)*

## About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1200 legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**