ITUWTSA NEW DELHI 2024

Digital India Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Full Member
Operational Member
Accredited Member
Global Research Partner
Associate Partner

Directions by CERT-In under Section 70B, Information Technology Act 2000

Guidelines on Information Security Practices for Government Entities

Technical Guidelines on SOFTWARE BILL OF MATERIALS (SBOM) NEW

ABOUT CERT-In
- Client's /Citizen's Charter
- Roles & Functions
- Advisory Committee
- Act/Rules/Regulations
- Internal Complaint Committee (ICC)
- RFC2350
- Press
- Tender
- Subscribe Mailing List
- Contact Us

REPORTING
- Incident Reporting
- Vulnerability Reporting
- Feedback

KNOWLEDGEBASE
- Guidelines
- Presentations
- White Papers
- Annual Report

RECRUITMENTS NEW

Security Tips for Common Users NEW

ADVISORIES

VULNERABILITY NOTES

Home - Current Activities

CURRENT ACTIVITIES

Key recommendations for CERT-In empanelled auditing organisations to contribute in & enhance the cybersecurity audit ecosystem

Original Issue Date:October 01, 2024

i. Auditing organizations should include an executive summary for board members & top management in all audit reports, translating the technical findings into relevant business risks and the overall security posture of the audited application or infrastructure.

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

iii. Organisation 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. Organisations may refer the method of verification document "Method of verifications to compliance with CERT-In Directions issued on 28.04.2022" shared over email and also available on CERT-In website at https://cert-in.org.in/PDF/Methods_of_Verification.pdf.

iv. During application audits, auditing organisation should check the compliance of the guidelines document "Guidelines for Secure Application Design, Development, Implementation & Operations" issued by CERT-In and available on CERT-In website and findings along with relevant evidences should be included in the audit report.

v. The limited list such as top 10, top 25 should be avoided as audit criteria. Audit should include discovery of all known vulnerabilities based on the comprehensive standards/frameworks like ISO/IEC, Cyber Security Audit Baseline Requirements, Open Source Security Testing Methodology Manual (OSSTMM3), OWASP Web Security Testing Guide along with applicable regulatory framework and directions & guidelines issued by agencies such as CERT-In.

vi. It is recommended that audit-related artefacts, such as hash values, versions, and timestamps should be captured & included in the audit certificate and reports.

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

viii. Audit report should be of highest standard 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. 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.

x. The audit certificate 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 certificate must explicitly state that the audit was not conducted on production environment.

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

xii. There will be a continuous performance assessment of the empanelled auditing organisations by CERT-In and organisations not meeting the desired criteria will be de-empanelled from the list.

xiii. Continuous capacity building for both technical staff and senior management of the auditing organisation in field of emerging domains & technologies should be developed and maintained.

xiv. Audit related data submitted to CERT-In is used for interventions at various levels to improve the cyber security posture of entities operating in Indian cyber space. Hence, empanelled auditing organisations must adhere with the data submission requirements to ensure the timely & accurate submission of audit metadata & audit reports to CERT-In.

xv. Empanelled auditing organisations are encouraged to share the information about their cybersecurity initiatives with CERT-In for value addition and disseminate it to boarder community.

Disclaimer

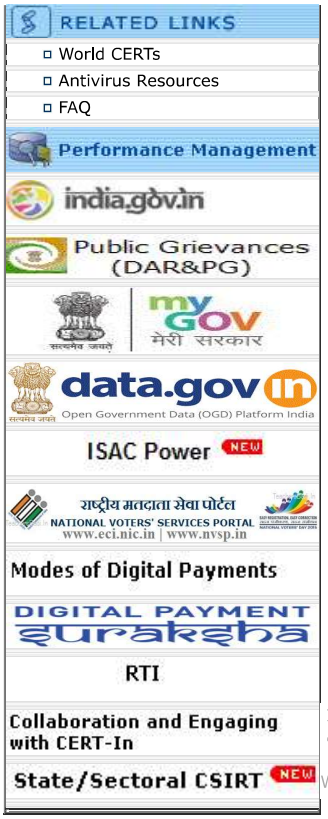
The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email:info@cert-in.org.in
Phone: +91-11-22902657

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India



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

Last Updated On October 07, 2024