

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 463
TO BE ANSWERED ON: 22.07.2026

INFORMATION SECURITY AUDITING ORGANISATIONS

463. SHRI BASTIPATI NAGARAJU:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the details of Information Security Auditing Organisations empanelled by CERT-In (Indian - Computer Emergency Response Team) for conducting vulnerability assessment, penetration testing and other security audits, State-wise;
- (b) the number of cybersecurity risks, vulnerabilities or non-compliances identified through the audits conducted for the banking sector between 2021 to 2025, year-wise;
- (c) the details of the efficacy of such audits including whether CERT-In has conducted any assessment of improvements in cybersecurity posture, reduction in incidents or compliance levels following these audits;
- (d) whether the Government proposes to expand the empanelled auditor network or revise audit guidelines to strengthen cybersecurity in the banking sector; and
- (e) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (e): The Indian Computer Emergency Response Team (CERT-In) has empanelled 237 information security auditing organisations to support and audit implementation of Information Security best practices across country. The State-wise distribution of these empanelled auditing organisations is given below:

S No	States/UT's	Nos
1	Andhra Pradesh	3
2	Chandigarh	1
3	Delhi	20
4	Gujarat	14
5	Haryana	16
6	Jharkhand	2
7	Karnataka	31
8	Kerala	10
9	Madhya Pradesh	1
10	Maharashtra	77

11	Punjab	1
12	Rajasthan	2
13	Tamil Nadu	24
14	Telangana	6
15	Uttar Pradesh	21
16	Uttarakhand	1
17	West Bengal	7
Total		237

A total of 34,017 cyber security audits were conducted by CERT-In empanelled auditing organisations for the banking sector during the period 2021–2025. The year-wise breakup is given below:

Year	No of Audits
2021	3,121
2022	4,010
2023	6,935
2024	7,732
2025	12,219
Total	34,017

CERT-In empanelled information security auditing organisations are consulted frequently by the entities in banking sector for their auditing requirements. The vulnerabilities identified by the empanelled organisations during the initial audits are addressed by the respective entities through appropriate remediation measures, including patching and mitigation. Subsequently, the auditing organisations conduct revalidation audits to verify the effective closure of the identified vulnerabilities and assess compliance with the prescribed cybersecurity requirements and recommendations.

CERT-In has taken following measures to improve cyber security posture through audits:

1. CERT-In has issued the “Comprehensive Cyber Security Audit Policy Guidelines” with the strategy to carry out cyber security audits in a consistent, effective, and secure manner across sectors including critical infrastructure.
2. CERT-In conducts regular interaction sessions with auditing organizations, such as “SAMVAAD” annual conference to strengthen the national cybersecurity audit ecosystem and bolster cyber resilience through knowledge sharing and regulatory alignment.
3. CERT-In has issued Guidelines for “Secure Application Design, Development, Implementation & Operations” for the entities engaged in developing or outsourcing application development.
