Ref. No.- 3(15)/2004-CERT-In (Vol. XIII) – Pt.
Government of India
Ministry of Electronics and Information Technology
Indian Computer Emergency Response Team (CERT-In)

Subject: Record of Discussion (RoD) of the interaction sessions held with CERT-In empanelled auditing organisations on 27-05-2023 at CERT-In, Shastri Park, Delhi.

CERT-In conducted the interaction sessions with empanelled auditing organisations at Shastri Park office on 27-05-2023 to discuss (i) Opportunities for improving audit qualities & audit outcomes, (ii) Challenges faced by auditee organisations, (iii) framework to improve quality of audits comprising enable & understand with deter & punish matrix, and (iv) continuous monitoring of audit performance of empaneled auditing organizations through application of data science by CERT-In.

2. The sessions were chaired by DG CERT-In. Officials of CERT-In and Head / Top management of CERT-In empaneled auditing organizations attended the interactions.

3. All empanelled auditing organisations i.e. 150 organizations were invited in 02 batches. The discussion was scheduled from 10:00 AM to 12:30 PM for the 1st batch and 02:00 PM to 04:30 PM for the 2nd batch.

4. DG, CERT-In welcomed the representatives of empanelled organisations and highlighted that most of empanelled organisations recorded excellent growth & maturity over time in quality of audits; coverage to diversified sectors & service offering of different audit types; and acknowledged the organizations who assisted, collaborated & shared information proactively with CERT-In. Further, DG, CERT-In addressed the participants on various concerns & issues, such as ensuring quality audits, actions in case of adverse feedback, timely submission of audit data to CERT-In and maintaining situational awareness on threat landscape & CERT-In initiatives, directions & regulations.

5. Empanelment team of CERT-In made a detailed presentation on key concerns, adverse feedback & observations, performance monitoring framework, deter & enable matrix. Following are the highlights of the session:

a) Organisation should ensure timely & accurate submission of quarterly audit data as same is used by CERT-In to have visibility and intervention in sectors & area of concerns.
b) Standards / references for audit should not be limited to lists such as top 10, top 25. Audit should include discovery of all known vulnerabilities based on comprehensive framework and standards like ISO/IEC, Cyber Security Audit baseline requirements, OWASP web security testing guide, Application security verification standards along with applicable regulatory framework and directions issued by CERT-In and other agencies.
c) Situational & context awareness on threat landscape, including CERT-In guidelines / initiatives should be maintained and used by auditing organizations in conducting audits.
d) Organisations should develop in-house audit quality assurance mechanism.
e) Organisations should ensure deployment of adequate & capable resources to conduct audits.
f) CERT-In empanelment should only be used for information security auditing engagements and organisations should not use empanelment status for other engagements.
g) Empanelled organisation should not engage in activities like digital break-in, sub-letting, violating terms & conditions of empanelment and unethical business transactions.
h) Framework to improve quality of audits and performance evaluation of empanelled auditing organisations are shared by CERT-In to the empanelled auditing organisations.
i) Audit Report should be of highest standard and comprehensive to include all details of audit, tools, manual process, findings, prioritization, sampling decisions, manpower involved & exemptions.

6. During the open floor session, auditing organisations highlighted various issues & challenges in conducting audits, key points were as follows:

a) Nature, scope and extent of audit is not defined properly by auditee organizations.
b) Applications are not developed using secure development & coding practices.
c) Lack of in-time actions by auditee organisation / developer in order to patch the vulnerabilities highlighted in audits.
d) Hindsight evaluation of auditing organization's performance is not appropriate for the purpose of incident attribution.
e) Audit should not be taken as compliance activity or just for sake of safe to host certificate. Auditee management should ensure adequate independence of auditing organization. Payments related conditions, if linked to patching & closer of

vulnerabilities, which are not in scope of auditing organizations, may hamper the audit independence.

f) Version control, change management & hash value are not maintained properly by auditee organizations.

7. Based on the deliberations, suggestions & issues highlighted by empanelled auditing organizations, following are proposed with the objective to improve the quality of audits:

a) CERT-In will adopt the framework to improve quality of audits comprising enabling actions as well as deter & punish mechanism. Framework is placed as Annexure-I.

b) In case of any genuine adverse feedback from auditee organisation/Agencies or any lapses in audit assignments are observed / reported by / to CERT-In, actions such as De-empanel by CERT-In, Penal & Legal Actions, blacklisting by auditee organization will be initiated against empaneled auditing organizations as per the framework without any reminder or notice.

c) In case of lapses (in terms of (i) within deadline and (ii) accuracy & completeness) in submission of quarterly audit data to CERT-In, defaulting auditing organizations will be de-empanel without any reminder or notice.

d) CERT-In will conduct at least one interaction session in a year for the top management and 2 sessions in a year for CISOs / Operational / Technical team.

e) CERT-In through application of data science may evaluate performance of auditing organizations and performance score will be considered for deciding on (i) eligibility for maintaining empanelment status of auditing organizations; and (ii) Maturity Grading for allotment in classes (e.g. class A, class B). Maturity grading of organization's performance and different maturity classes will be hosted in public domain (CERT-In website) for transparency.

f) Mechanism to generate unique audit number for each audit conducted by empaneled auditing organization may be explored by CERT-In.

g) Version, change history, hash value and other evidences of the audited application/infrastructure should be collected & maintained by auditing as well as auditee organizations.

h) Audit Report should be comprehensive and factual with all details & evidences of audit, tools, manual process, findings, prioritization, sampling decisions, manpower involved & exemptions.

Interactions ended with vote of thanks to all empanelled auditing organisations.

Annexure-I

Framework to improve quality of audits

I. **Enable & Understand:** CERT-In will conduct regular conference / interaction with all auditing organizations to share concerns and observations & actions in case of adverse feedback. Effort is expected to build trust and identification of opportunities for improvement.

II. **Deter & Punish:** Following graded actions will be taken by CERT-In and auditee organization in case of adverse reports and poor quality of audits:

a) Warning & Written Commitment
b) Move to Watch List
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 impact), First adverse report includes missing of maximum 2 vulnerabilities, conflict with auditee, first instance of noncompliance to CERT-In data collection framework, etc	CERT-In to issue show cause and obtain corrective action report from Auditing Organisations with issue warning along with written commitment.
2.	Suspension	1. Adverse feedback from Auditee regarding technical competency auditor's attributes etc.	Suspension to be revoked based on satisfactory submission of Corrective

		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	Actions and witnessing, if needed
3.	Withdrawal of Empanelment	Auditing malpractices, Sub-standard 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