



EC No. 307/DoS-25/2024

Ref. No. NB.HO.DoS.CSITE/ 3300 / CS-01 /2024-25

17 December 2024

1. The Chairman, all Regional Rural Banks
2. The Managing Director/Chief Executive Officer, all State Central Cooperative Banks
3. The Managing Director/Chief Executive Officer, all District Central Cooperative Banks

Madam/Dear Sir

Conduct of Information Technology/Cyber Security Audit

As you may be aware, there has been an increasing number of cyber incidents and attacks that require all systems to be alert and vigilant regarding potential threats. This is primarily due to the existence of vulnerabilities in software, applications, websites and configurations of IT infrastructure. Moreover, due to application of emerging technologies such as Artificial Intelligence/ Machine Learning, Internet of Things, etc. threat vectors are evolving and becoming more complex.

2. In the circumstances, as advised by the Ministry of Electronics and Information Technology (MeitY), Government of India, we advise as under:

(i) In order to take preventive measures and minimize the security risk & exposures, all Supervised Entities of NABARD (viz. State Cooperative Banks, District Central Cooperative Banks and Regional Rural Banks) should get their IT infrastructure, websites and applications (including APIs) audited on a regular basis or whenever there are any changes/updates in infrastructure or websites/applications.

(ii) Audits should be conducted against comprehensive frameworks and should follow MeitY/CERT-In Guidelines released/updated from time to time (enclosed). The list of empanelled agencies who can do the cyber security audit is available at: <https://www.cert-in.org.in/PDF/Empanel.org.pdf>.

राष्ट्रीय कृषि और ग्रामीण विकास बैंक

National Bank for Agriculture and Rural Development

पर्यवेक्षण विभाग

प्लॉट नं. सी-24, 'जी' ब्लॉक, बान्द्रा - कुर्ला कॉम्प्लेक्स, बान्द्रा (पूर्व), मुंबई - 400 051. • टेलि.: 022 6812 0039 • फैक्स : +91 22 2653 0103 • ई-मेल : dos@nabard.org

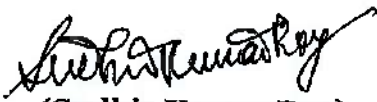
Department of Supervision

Plot No. C-24, 'G' Block, Bandra-Kurla Complex, Bandra (E), Mumbai - 400 051. • Tel.: 022 6812 0039 • Fax : +91 22 2653 0103 • E-mail : dos@nabard.org

3. You are, accordingly, advised to immediately put in place a system of regular conduct of cyber security audit through CERT-In empanelled agencies strictly as per the MeitY/CERT-In guidelines atleast on an annual basis or whenever there are any changes/updates in infrastructure or websites/ applications, in consultation with the Board of Directors of your bank.
4. In case of third party hosting service provider, the instructions given at para F of the guidelines may be followed which provide that in case a services/website is hosted on a webserver owned by another organization, the webserver system, its operating system and webhosting application software including backend database application software, if any, are under the control of the organization hosting the website (i.e. owning the webserver) and it is the responsibility of webserver owner to take care of information security auditing of these, as the organization owning the website contents does not have any access or control over these assets. However, since the data/software related to the website are under the control of the organization owning the contents of the website, their responsibility is limited to get these audited by a CERT-In empanelled information security auditing organization. In such cases, compliance may be obtained from the third-party hosting service provider.
5. The copies of Audit Reports along with information in the enclosed format may please be submitted to NABARD at csite@nabard.org on a quarterly basis by the last working day of the quarter to enable us to keep MeitY, Govt of India timely informed of the same.

Please acknowledge.

Yours faithfully


(Sudhir Kumar Roy)
Chief General Manager

Encl. : As above

FORMAT

Report for the quarter ended _____ (to be submitted by last working day of the last month of the quarter)

1. Name of the Supervised Entity (SE): _____
2. Cyber security audit conducted on _____ (copy of report enclosed)
3. Name of third-party hosting service provider: _____
4. Name of the agency which had conducted cyber security audit: _____
5. Whether agency at 4. empanelled by CERT-In: _____
6. Type of audit, audit scope, methodology/standards :
7. Summary:

Sr No	Particulars	SE's comments
7.1	Major recommendations mentioned in audit report	
7.2	Status of action taken/closure status in respect of each such recommendation	
7.3	Significant cyber security audit recommendations (outlining the overall major recommendations which interalia include policy enhancement, access control improvements, third party risk management, incident response preparedness, training and awareness, etc.)	
7.4	Whether fully/partly complied with CERT-In/MeitY guidelines	
7.5	Whether fully/partly complied with Cyber Security Framework Guidelines of RBI/NABARD	



Handling Computer Security Incidents

Indian Computer Emergency Response Team

IT Security Auditing

Guidelines for Auditee Organizations

Version 5.0

A. INTRODUCTION

IT Security auditing is a critical component to test security robustness of information systems and networks for any organization and thus the selection of the most appropriate IT security auditor is a complex decision. IT security auditing is often considered for outsourcing owing to its highly specialized and technical nature. Considering the involvement of sensitive and confidential organizational data, it is vital that IT security auditor be capable and trustworthy.

IT Security auditing assignments can take many different forms depending upon the type and size of auditee organization. It is suggested that audit contracts be finalized only upon consultation with auditee's legal/contractual experts and after negotiations with the auditor. IT security auditing can be conducted as a separate activity or as part of the risk assessment process under the risk management program.

B. AUDIT COMPONENTS AND CHARACTERISTICS

The auditor will need clear and unambiguous direction from auditee management (written rules of engagement), clearly defined scope for security audit and input on what is required for planning & assessment, requirement analysis, test execution & analysis, results and documentation.

B.1 Introduction

Identifies the purpose, participants (auditee & auditor organization and any other), technical team (both auditee and auditing organization), briefing schedule and audit scope definition.

B.2 Audit Environment

Describes the environment in which the auditor will perform the audit including the physical location, hardware/software being used, policy and procedures the auditor will need to follow. Key components are:

- 2.2.1 Entities and Locations
- 2.2.2 Facilities at each location
- 2.2.3 Equipment at each location
- 2.2.4 Policies, Procedures and Standards
- 2.2.5 Agreement and Licenses

B.3 Roles and Responsibility

In case any of the activities to be audited in the auditee organization are outsourced, auditee must ensure that relevant personnel from outsourced organization are available at the time of audit. The auditor's responsibilities need to articulate not just the audit tasks, but also the documentation of their activities, reporting their actions and *modus operandi*.

Please Note:

"Auditing Man day" shall mean auditing effort (both on-site as well as off-site) of minimum 8 hours, excluding breaks, by a person with suitable auditor qualification such as CISA/CISSP/BS 7799 Lead Assessor/ISA or any other formal security auditor qualification.

B.3.1 Auditor Organization Responsibilities: The contract should include clear identification of the following:

B.3.1.1 Audit Checklist (Mutually agreed upon by the Parties)

B.3.1.2 Audit Plan with timelines (Mutually agreed upon by the Parties)

B.3.1.1 Audit tasks

B.3.1.2 Documentation requirements

B.3.1.3 Audit Support requirements

B.3.1.4 Reporting Requirements: Structure, Content and secure handling of final deliverable (Such as Audit Reports) should be mutually agreed by the auditee and auditing organization.

B.3.1.5 For critical and government sector organizations, Auditor must only deploy the manpower with background verification check done from suitable Law Enforcement Agency.

B.3.2 Auditee Organization Responsibilities: Besides the conditions that get specified in the contract, the following form part of auditee obligations:

B.3.2.1 Auditee refrains from carrying out any unusual or major network changes during auditing/testing.

B.3.2.2 To prevent temporary raise in security only for the duration of the test, the auditee notifies only key people about the auditing/testing. It is the auditee's judgment, which discerns who the key people are; however, it is assumed that they will be people at policy making level, managers of security processes, incident response, and security operations.

B.3.2.3 If necessary for privileged testing, the auditee must only provide temporary access tokens, login credentials, certificates, secure ID numbers etc. and ensure that privilege is removed after the audit.

B.3.2.4 A Technical team should be assigned as point of contact by the auditee organization for assisting and monitoring the auditors during the audit and the details of the technical team should be shared with the concerned auditors. Auditee should assure and schedule regular interaction of technical team with auditors.

B.3.2.5 A Formal Confidentiality & Non-disclosure agreement must be signed with the auditor before starting of the work.

B.3.2.6 There should be a well defined escalation matrix both for the auditee and auditing organization for addressing any problem encountered during the audit process which should be shared with respective authorities.

B.3.2.7 A well defined mechanism must be in place which clearly states the procedure in which the report would be stored and destroyed after the completion of audit by the auditing organization. Thus, the mechanism should be designed in such a way that it confirms the following:

- Secure handling of report and data at transit.
- Secure handling of report and data at rest.
- Disposal time of report and related information by auditor.

B.4 Terms and Adjustments

This section provides details about:

B.4.1 Costs

B.4.2 Periods of Performance with Deliverables and Timelines

B.4.3 Dispute Resolution

B.4.4 Remedies for Non-Compliance

B.4.5 Maintenance of Agreements

C.AUDITEE EXPECTATIONS

The following are the expectations of auditee organization from an auditor:

- C.1 Verifying possible vulnerable services only with explicit written permission from the auditee.
- C.2 Auditors must verify the existing policies of the organization against the industry standards and best practices and suggest the necessary improvements if required.
- C.3 Refrain from security testing of obviously highly insecure and unstable systems, locations, and processes until the security has been put in place.
- C.4 A formal Confidentiality & Non-disclosure agreement should be signed by the IT Security auditing organization prior to commencing the cyber security auditing work. The auditing organization and its auditors are ethically bound to maintain confidentiality, non-disclosure of auditee information, and security testing results.
- C.5 Auditing organizations must comply with all applicable regulations, acts/Circulars from Government & Regulators with respect to data security & privacy.
- C.6 The security auditor always assumes a limited amount of liability as per responsibility. Acceptable limited liability could be equal to the cost of service (this includes both malicious and non-malicious errors and project mismanagement).
- C.7 Clarity in explaining the limits and dangers of the security test.
- C.8 In the case of remote testing, the origin of the testers by telephone numbers and/or IP addresses is made known and a formal written permission with a clear definition of the tasks to be performed should be taken.
- C.9 Seeking specific permissions for tests involving survivability failures, denial of service, process testing, or social engineering.
- C.10 The scope is clearly defined contractually before verifying vulnerable services.
- C.11 The scope clearly explains the limits of the security test.
- C.12 The test plan includes both calendar time and man-hours.
- C.13 The test plan includes hours of testing.
- C.14 The security auditors know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the customer organization and the result of such testing should be approved formally by the authorized person of auditee organization.
- C.15 The exploitation of Denial of Service tests is done only with explicit permission.
- C.16 Social engineering and process testing are performed in non-identifying statistical means against untrained or non-security personnel.
- C.17 Social engineering and process testing are performed on personnel identified in the scope and may not include customers, partners, associates, or other external entities.
- C.18 High risk vulnerabilities such as discovered breaches, vulnerabilities with known, high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may put immediate lives at risk, discovered during

testing are reported immediately to the customer with a practical solution as soon as they are found.

- C.19** Refrain from carrying out Distributed Denial of Service testing over the Internet.
- C.20** Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.
- C.21** Notify the auditee whenever the auditor changes the auditing plan, changes the source test venue, has high risk findings, previous to running new, high risk or high traffic tests, and if any testing problems have occurred. Additionally, the customer is notified with progress updates at reasonable intervals.
- C.22** Reports include all unknowns clearly marked as unknowns.
- C.23** All conclusion should be clearly stated in the report with the clear objective evidence for each conclusion drawn.
- C.24** Reports use only qualitative metrics for gauging risks based on industry-accepted methods.
- C.25** Auditee is notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
- C.26** All communication channels for delivery of report are end to end confidential.

D. GENERAL GUIDELINES

- D.1** Auditee must implement the guidelines and advisories issued by CERT-In and/or suitable Government Agency time to time in their auditing program.
- D.2** Regular interaction framework during audit should be setup.
- D.3** Auditee organizations need to verify the technical credentials of the manpower deployed for the audit at their end in line with the qualification requirement mentioned at "Guidelines for applying for Empanelment" and auditee should interview manpower deployed by auditor for conducting the audit.
- D.4** Auditee will ensure from Auditor that audit related data should be stored only on systems located in India with adequate safeguards.
- D.5** Ensure that auditor is utilizing industry standard methodologies, best practices for security testing.
- D.6** Scope of audit (in case of VA/PT) should not be limited to the few lists like OWASP top 10 or SANS Top 25 programming errors, it must include discovery of all known vulnerabilities.
- D.7** Auditee must demand for the working notes upon completion of the audit (provisions for this must be made in the audit contract itself) and should ask for audit evidences collected to be submitted as appendix along with the final audit report.

Indian Computer Emergency Response Team

- D.8** Audit report format should be mutually agreed upon (Auditee and Auditor) and finalized before commencement of the audit. A sample web-application audit report for reference is available at Annexure-I.
- D.9** Regular meetings should be held between the auditor and auditee representatives (SPOCs) to review the progress of the audit in order to assess and improve the audit efficiency.
- D.10** Auditee must ensure that the tests agreed upon in the audit contract are actually being conducted by the auditor and also that the prescribed timeline is being followed, through the aforementioned meetings.
- D.11** CERT-In empanelled auditors are selected after much scrutiny and testing but it is vital to understand that while the list of empanelled auditors is true and accurate, CERT-In cannot guarantee the authenticity of audit details provided by these organizations.
- D.12** While selecting an auditor, it is the responsibility of the auditee to check the domain of audit conducted, previous audits conducted and other relevant details. An auditee should have a clear understanding of the auditor's audit methodology, tools used, experience in the relevant domain and all available alternatives like other competent organizations before selecting.
- D.13** If the credibility of the auditor is unclear, auditee must make sure that the contractual agreement allows the auditee to stop the audit and choose another auditor within a reasonable duration of time in order to avoid financial losses on both ends.
- D.14** Feedbacks/complaints to CERT-In help improve the quality of selecting auditing organizations in future, thus, it is both an auditee's right and duty to provide relevant feedbacks. All feedbacks/complaints are kept confidential and are acted upon promptly with utmost importance.
- D.15** Last but not least, the auditee must act upon the relevant audit findings and strive to improve the IT security.
- D.16** Auditee Organisation are required to verify credentials of CERT-In empanelled organisation, before availing their services, by checking their details in the list of CERT-In empanelled information security organisations.
Don't fall prey to fake organisation posing as CERT-In Empanelled Information Security Organisation.

E. SNAPSHOT INFORMATION & TECHNICAL MANPOWER DETAILS

Information about the CERT-In empanelled Auditing organization is available at CERT-In website.

Indian Computer Emergency Response Team

The information provided on the CERT-In website can help the auditee organization with respect to the following:

- Evaluation of man power and skillset details of an auditing organization
- Experience of an auditing firm relevant to information security audits
- Categories of information security audit conducted by the auditing organization
- Information security audits carried out by an organization in last 12 months (sector wise)
- Category wise number of audits conducted by an organization in last 12 months
- Technical man power deployed for audits by an organization with details
- Tools used in various audit

NOTE -Snapshot information available at CERT-In website is as provided by the respective organizations. The Information is not verified by CERT-In and thus CERT-In does not hold any responsibility in case of any discrepancy found in the information.

F. THIRD PARTY HOSTING SERVICE PROVIDER

In case a services/website is hosted on a webserver owned by another organization, then the webserver system, its operating system and webhosting application software including backend database application software, if any, are under the control of the organization hosting the website (i.e. owning the webserver) and it is the responsibility of webserver owner to take care of information security auditing of these, as the organization owning the website contents does not have any access or control over these assets.

However, since the data / software related to the web-site are under the control of the organization owning the contents of the website, their responsibility is limited to get these audited by a CERT-In empanelled information security auditing organization.

The organization, owning the website contents, can select any auditing organization out of the CERT-In empanelled information security auditing organizations as per their office rules & procedures and financial guidelines to get these audited. The information security audit report from the information security auditor should clearly state that these webpages, including the backend database and scripts, if any, are free from any vulnerability and malicious code, which could be exploited to compromise and gain unauthorized access with escalated privileges into the webserver system hosting the said website.

E. RELATIONSHIP AUDITEE & AUDITOR

Auditing process is aimed for the continual improvement of the auditee organization and thus the auditor perspective should be aimed at refining the security process rather than

Indian Computer Emergency Response Team

merely complying with the standard against which the auditing is done. The Auditing organization must maintain a relationship with the auditee even after the completion of the audit process to keep auditee organization updated for the latest security developments and to help in implementing the secure environment.

G. DISCLAIMER

The outline provided here must be treated only as a guide/standard format by the auditee; the specific formats and terms & conditions of auditors will be unique for each organization.



Indian Computer Emergency Response Team

Annexure-I

Sample Report Format for Web-application Security Audit

Audit Conducted for (Name of Auditee Organisation):

Audit Conducted by (Contact Person details with email and mobile):

Report Submitted On (Date):

Test duration: From (Date) To (Date) _____

URL/IP addresses of the Web-Application:

Report Reviewed by:

Report Handed over to (Name and contact details of person from auditee organization):

I.Executivesummary:

Section-I

<Overview of scope, audit methodologies, tools used, observations, etc. >

Section-II

List of vulnerable points

<Separate table for each IP tested>

IP Address with URL <Description of machine (IP/OS/Services running)>

S.no	Vulnerable point/Location	Vulnerability	Mean of identification Manually/Tool (if tool mention the name)

II. Vulnerability Assessment:

Section-I

<Separate section for each IP>

IP with URL : *<details of machine IP/OS/ services>*

<for each vulnerable point>

Vulnerable Point-1/2/3..../n

- a. Vulnerable Point:
- b. Name of Vulnerability:
- c. Steps of verification of vulnerability(Proof of concept) with screenshots:

Section-II *<if penetration testing is in scope>*

<for each penetration>

Penetration-I/II/III/IV:

Machine Detail: *<IP/URL/OS/Service>*

Vulnerabilities used for exploitation:

Proof of concept with screenshots: *<Step by Step- detail description of Penetration>*



Indian Computer Emergency Response Team

Details of Team engaged for audit:

S.No.	Name	Email and phone	Qualification and certification



Indian Computer Emergency Response Team

Guidelines for CERT-In Empanelled Information Security Auditing Organizations Version 3.0

People

- Are courteous, cooperative, and professional.
- Have undergone a background check before employment. In case of employees moving from one CERT-In empanelled organization to another, a NOC / Relieving Letter shall be required from the previous organization as part of background check.
- For Government and critical sector audits, Organization must deploy manpower declared to CERT-In in snapshot information form. CERT-In reserves the right to verify/audit such information independently or from the auditing organization or the auditee organization.
- Have adequate competency in
 - security technology
 - security processes
 - security controls
 - security trends
 - fact collection
 - reporting
- Have high ethics and morals.
- Have experience and maturity in interacting with senior management and creating trust.
- Understand the consequences of their actions.
- Understand and ensure there is no conflict of interest.
- During and after the audit assignment are aware of information classification and know how to maintain confidentiality, security and privacy (such as collection, use, release, disclosure) of information and audit including but not limited to protecting against theft and damage of such information.
- Have signed Non-disclosure agreement(NDA) with the organization at the time of joining
- May need to sign NDA with the auditee organization depending upon the requirement of project under information to its employer organization.

Technical

- Auditors should help auditee organization in identifying the scope of work.
- Auditors must utilize industry standard methodologies, best practices for security testing. Solely tools based testing should be discouraged.

- Auditors should deploy a verification team (Red Team) to verify the work performed by their audit team (White Team).
- Auditor should clearly mention the environment in which the web application/ application has been tested in case of web application/ application security audit.
- Auditor will be required to audit and test the website on the staging server/testing environment provided by hosting service provider before issuing the audit certificate.
- Structure and Contents of final deliverable of the audit/testing (like vulnerability assessment report) should be finalized with the auditee organization before commencement of project.
- Refrain from carrying out Distributed Denial of Service testing over the Internet.
- Refrain from any form of flood testing where a person, network, system, or service, is overwhelmed from a larger and stronger source.
- Refrain from testing and exploiting high risk vulnerabilities such as discovered breaches or which may put immediate lives at risk.
- Ensure appropriate approvals have been received in writing prior to carrying out any penetration tests and installation of tools and install tools in the presence of auditee system administrator.
- Ensure removal of tools after the completion of task and do not install any other software or damage any existing auditee software. Get acceptance of auditee for removal of tools in the presence of auditee system administrator.
- Ensure you provide a list of tools planned to be installed to auditee and provide a written confirmation to the auditee that you are not violating any IPR or license norms while using and installing the tools.
- Auditee related data should only be retained for specific period of time as in agreement with the auditee and disposed-off as per defined & agreed process. The collection, preservation and disposal of data collected by the auditor should be in accordance with the agreement entered between Auditor & Auditee. Auditor will ensure there is no mirroring of data outside the country. In any case, the auditor will not leak data at any time (during or after the audit) to any third party without the permission of Auditee. After wiping the data, auditing organization should also make sure that data cannot be retrieved by any known forensic technique.

Process

- Ensure a Formal Non-disclosure agreement is signed with the auditee and is in place prior to start of work.
- With or without a Non-Disclosure Agreement contract, the security auditor is ethically bound to confidentiality, non-disclosure of auditee information, and security testing results.
- Ensure that the timelines and commitments made to the auditee are adhered to.
- Ensure that there is no “expectation gap” in conducting an audit. The “expectation gap” is the difference between what perceive an audit to be and what the audit profession claim. Reduce or eliminate this by explaining in detail upfront the audit process, collection of artifacts and deliverables.
- All the observations made during the audit are well supported with objective evidences and all evidences are compiled carefully and correctly with the report.
- All the evidences gathered during the process of audit are presented in a manner that the decision makers are able to use them effectively in making credible risk based decisions.
- Audit report should mention appropriate timelines for closure of vulnerabilities according to severity.
- The security and confidentiality of the auditee data should be managed effectively and well established procedures should be defined and documented to handle auditee data during and after the audit.
- The information regarding audit team selected for conducting audit should be shared with the auditee and a documented approval regarding the same should be procured before the formal commencement of audit.
- CERT-In reserve the right to seek/audit information from auditing organizations for any project done within the time frame of empanelment period.
- Ensure that suggested controls and remedies are practical and implementable.
- Request auditee to provide feedback on the audit conducted to CERT-In as well as to you on completion of the audit.
- Ensure that CERT-In is not made a part of any contract between auditee and auditor.

- Be aware that CERT-In can be a part of the audit team to assess the quality and maturity of audit, if it so desires and the same should be communicated to the auditee.
- Auditor shall not use the CERT-In logo, nor make any reference to the Auditors association with CERT-In on any publicity material, promotional material or product without the prior written permission of CERT-In. Before CERT-In examines requests for permission, the Auditor shall submit the wording and presentation of such information.
- An Auditor may use the words "This Organization is empanelled by CERT-In for providing information Security Auditing Service". No other words shall be used to describe the Auditors relationship with CERT-In without the prior written permission of CERT-In.
- The Auditor shall not use the CERT-In logo in any circumstances that would bring the Audit Service or CERT-In into disrepute.
- The Auditor shall indemnify, and keep indemnified CERT-In against all claims, demands, actions, costs, expenses, (including without limitation, damages for any loss of business, business interruption, loss of business information or other indirect loss), arising from or incurred by reason of any third party claims against CERT-In relating to or arising from the performance or non-performance by the Auditor of any or all of its obligations under this terms and conditions as well as his Contract with the auditee.
- Provide quarterly report to CERT-In regarding generic information related to information security audits, number of audits carried out, the sector in which the audit has been carried out, the high level findings, new areas emerging for audit.
- It is responsibility of empanelled organization to keep CERT-In updated with snapshot information.
- Ensure to maintain a regular contact with the auditee after the audit has been completed and assignment is over, as a good business relationship. Auditors should setup a communication channel to inform/alert auditee about information security related latest development feasible to auditee environment.
- Auditee related data should be stored only on systems located in India with adequate safeguards and should keep the auditee informed of the means & location of storage and seek auditee's consent where necessary. During project engagement, audit related data should be kept in encrypted form in auditor's laptop. Auditing organization should also ensure that data is wiped from auditor's laptop after completion of the project.
- The sharing and disclosure of auditee related data, where necessary, should only be done with prior consent of auditee organization. The auditee/project related data should not be shared with or disclosed to any overseas partner, unless specifically authorized by the auditee.

- The audit outcome & related matters should only be communicated to the specified Point of Contact (POC) of the auditee organization. The audit outcome should only be shared using secure methods such as use of passwords, encryption etc.
- Auditing organization should prefer only official email id for sharing of audit report/data with auditee.
- Organization should have Incident Management Policy and related processes in place with clearly defined escalation matrix and procedures to deal with non-compliance. This process for dealing with incidents should be shared with the auditee.
- In case of the incidents where client audit related data is leaked to unauthorized entity (intentionally or unintentionally) , the auditing organization should inform the auditee of incident and take all necessary actions to address the incident as may be required.

Template for Consolidated Cybersecurity Audit Report

(To be submitted by <Regulator> to Ministry of Electronics and Information Technology latest by 15th day of the succeeding quarter. For example, for Q1, the submission deadline is July 15th. The report should be in excel format)

Total Number of Entities under purview of <Regulator>:

Periodicity of Audit recommended by <Regulator>:

Is there Cyber Security Audit Guideline issued by <Regulator>:

Latest date of issuance of Cyber Security Audit Guideline by <Regulator>:

I. Summary of Audits:

< Action taken report on Audit Observations >

S.no	Name of Entity under purview of <Regulator>	Date of Last Audit Conducted	Name of Auditing Organisation	Type of Audit, Audit Scope, Methodology / Standards	Major Recommendations mentioned in Audit Report	Status of Action taken / Closure Status

II. Gaps and challenges observed in Audits:

III. Significant Cyber Security Audit recommendations:

< Outlines the overall major recommendations which inter alia include:

- a. Policy Enhancement
- b. Access Control Improvements
- c. Third Party Risk Management
- d. Incident Response Preparedness
- e. Training and Awareness etc. >

IV. Conclusion

<number> of entities out of <total_number_of_entities> are fully compliant to Cybersecurity Audit guideline issued by <Regulator>

<number> of entities out of <total_number_of_entities> are fully compliant to MeitY/CERT-In Audit Guidelines.

< Brief Action advised for other remaining entities to comply with Cybersecurity Audit guideline issued by <Regulator> >
