Methods of verification to compliance with CERT-In Directions issued on 28.04.2022

S. No.	Compliance requirements	Methods of verification
1	All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.	1) During an audit assignment, check whether the audited ICT infrastructure of the auditee organization is synchronized with the system clocks of designated NTP servers. Some of the possible verifications methods are mentioned below: i. Review system logs and audit trails to identify timestamps indicating synchronization events with the designated NTP servers. ii. Analyze network logs and traffic iii. Time Source Verification 2) It should be ensured that the time zone information is being recorded along with the time to facilitate accurate conversion when needed.
2	Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being	1) During an audit assessment, it may be ascertained and deduced whether there was any cyber incident as mentioned in Annexure I of the CERT-In directions dated 28.04.2022 had occurred but was not reported to CERT-

	brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969).	In within 6 hours of noticing, the same should be immediately brought to the notice of CERT-In. 2) If Incident Management functions is under scope of assessment then, it may be assessed whether policy or plan envisage reporting of cyber incidents to CERT-In in compliance with CERT-In directions and reporting requirements. 3) Requirement of incident reporting as per CERT-In directions needs to be communicated to auditee by auditing organizations. Same should be included as part of audit report.
3	Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration: a. Validated names of subscribers/customers hiring the services b. Period of hire including dates c. IPs allotted to / being used by the members	1) In case, auditee organization is a Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers or Virtual Private Network Service (VPN Service) providers, auditing organization should check, whether the following information of the subscribers is being maintained by organization for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration: a. Validated names of subscribers/customers hiring the services b. Period of hire including dates c. IPs allotted to / being used by the members

	d. Email address and IP address and time stamp used at the time of registration / on-boarding e. Purpose for hiring services f. Validated address and contact numbers g. Ownership pattern of the subscribers / customers hiring services	d. Email address and IP address and time stamp used at the time of registration / on-boarding e. Purpose for hiring services f. Validated address and contact numbers g. Ownership pattern of the subscribers / customers hiring services. 2) Below mentioned verification methods may be followed by the auditing organisations: i. Review of registration policies and procedures, ii. Review of registration forms or agreements to ensure auditee have provisions for collecting accurate subscriber information and the retention period for collected data, iii. Examine the organization's data retention policies, iv. Review audit trails and logs to verify compliance with data registration and retention requirements.
4	The virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by Ministry of Finance from time to time) shall mandatorily maintain all information obtained as part of Know Your Customer (KYC) and records of financial transactions for a period of five years	1) In case, auditee organization is virtual asset service provider, virtual asset exchange provider and / or custodian wallet providers (as defined by Ministry of Finance from time to time), auditing organization should check whether, all information obtained as part of Know Your Customer (KYC) and financial transactions are recorded & maintained for a period of five years.

		2) Auditing organisations may examine the organization's data retention policies for financial transactions and KYC information.
5	All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.	1) During an audit assignment, check whether the logging is enabled on the audited infrastructure and logs are being retained for rolling period of 180 days. 2) These can be verified by reviewing the auditee organization's policy documentation such as logging policies and procedures, assessing system configurations to ensure logging is enabled, and confirming that logs are retained for the specified duration. Additionally, audits can involve examining log storage practices to ensure compliance with requirements.
6	CERT-In Directions dated 28.04.2022	Compliance requirements of CERT-In directions needs to be communicated to auditee by auditing organizations. Same should be included as part of audit report.