S. No.	Domain	Parameters	Evidence/Supporting Document	Draft CEA Regulations 2025 - Relevant Clause	Mandatory (Immediate)/Relaxed (With Defined Time Window)/Not Critical (Can be Part of Next Round of Check)
1	Organizational & Governance	**CEO/CMD/MD/Top Management** (Key cybersecurity oversight authority for decision-making & accountability)	Cyber Security Governance/ Board/ Management Approval Note/ Appointment Letter/ Cyber or Information Security Steering Committee	**Chapter - III and Chapter V**	**Mandatory**
		Entity/Parent Company Details Name, Location, CISO, Alternate CISO, Contact Details	Cyber Security Organizational Structure/ Office Orders/ CISO Appointment Order/ Alt. CISO Appointment Order Note: The parent organization's CISO shall be accountable and responsible for cybersecurity across all plants, and it shall not be mandatory to designate individual plant-level CISOs; accordingly, the same CISO name may be reflected for all plants in the FTC checklist.	**Chapter - III and Chapter V**	**Mandatory**
		Plant Details Name, Location, Plant Capacity (MW), CISO, Alternate CISO, Contact Details	Cyber Security Organizational Structure/ Office Orders/ CISO Appointment Order/ Alt. CISO Appointment Order (If Plant Level CISO and/or Alt. CISO appointed, details should be given)	**Chapter - III and Chapter V**	**Mandatory**
		Information Security Division(ISD): Information Security Division should be defined	Dedicated Division: Each entity must establish an ISD, headed by the CISO. Sufficient manpower should be mainitained in ISD to ensure round the clock operations.	**Chapter - III and Chapter V**	**Mandatory**
2	IT/OT Infrastructure & Network Architecture	**Network Architecture, along with IT–OT convergence and exposure to Internet (Closure based on inspection visit)**	**Network Architecture Diagram** - Cyber Security Architecture Document - IT-OT Connectivity Defined - Mode of Convergence - One-way, Bi-directional, Air-gapped - DMZ Architecture Diagram	**Chapter - III**	**Mandatory**
		IT and OT Technology Architecture & Deployment (Closure based on inspection visit)	**Advance Level Security Technology Implementation:** Packet filtering & Deep Packet Inspection (DPI), Content, user & application-based filtering, Encrypted traffic inspection, Geo-fencing, Automatic signature & behavior updates, APIs Security, Web Application Firewall (WAF), Endpoint Detection & Response (EDR/XDR)	**Chapter - III**	**Relaxed (Within One Year)**
			Minimum Level Security Technology Implementation: Firewall Placement at Perimeter Level - Network Security Architecture, IDS/IPS Deployment, Antivirus Solution, Security Monitoring Architecture, SOC Architecture Document, SIEM use cases deployment and Monitoring , OEM & Model details, Provide end-of-life (EOL) / end-of-support(EOS) details for hardware/software.	**Chapter - III**	**Mandatory (Immediate)**
		ISO/IEC 27001 Certification	Compliance with and obtain ISO/IEC 27001 certification or an equivalent Technical Criteria Certificate covering all critical systems within one year from the date of plant commissioning. To maintain independence and avoid conflict of interest, no more than four consecutive certification audits for ISO/IEC 27001 or the Technical Criteria Certificate shall be conducted by the same auditing agency or personnel.	**Chapter - III**	**Relaxed (Within One Year)**
		Data Center (DC) & Disaster Recovery Center (DRC) (Closure based on inspection visit)	**Required Documents:** Business Continuity Plan (BCP), DR Drill Report,Data Centre Details(mode of deployment of technologies (IT and OT), ownership and management of servers, data transition/migration plan, the presence and location of data centres (primary and disaster recovery), access control mechanisms implemented (physical and logical) to ensure secure and authorized access)	**Chapter - III**	**Relaxed (Within One Year)**
3	National & Regulatory Compliance	**Cyber Swachhta Kendra (CSK) Onboarding**	**Required Documents:** CERT-In Compliance Declaration/ CSK Onboarding Proof/CERT-In Incident Reporting/Incident Reporting SOP The list of All public IPs onboarded with CSK.	**Chapter - III**	**Mandatory (Immediate)**
		NCIIPC and Critical Information Infrastructure (CIIs)	**Required Documents:** NCIIPC Communication Letter/CII Notification Order, NCIIPC coordination status CII declaration (Notified/Proposed), Asset Classification Register. CII / Protected Systems should be notified by NCIIPC within one year from the date of plant commissioning. During checklist verification, valid documentary evidence of certification progress/completion shall be reviewed. A formal undertaking confirming compliance with the requirement shall be submitted and duly signed by the CISO.	**Chapter - III**	**Relaxed (Within One Year)**
4	Cyber Resilience & Risk Readiness	**Cybersecurity Policy (CSP)**	**Required Documents: Cyber Security Policy (CSP):** Must be documented, approved, and reviewed annually. CSP should be maintained at the organizational level covering all plants from Day 1. The Policy should mentioned about Non –Disclosure Agreement (NDA) shall be included in Service Level Agreement (SLA) with the vendors engaged for critical applications and critical systems, manging sensitive information and data and cloud service provider to ensure the confidentiality, integrity and availability of such data and information, during their contract period as well as after completion of such contract thereof.	**Chapter VI**	**Mandatory (Immediate)**
		Cyber Crisis Management Plan (C-CMP)	**Required Documents:** The Cyber Crisis Management Plan (CCMP) vetted by CERT-In with the assistance of CSIRT-Power and maintained at the organizational level, covering all plants and operational units from Day 1. Incident Response Playbooks should be implemented and Reporting Timelines is within 6 hours It should include detailed Standard Operating Procedures (SOPs) for detection, identification, response, and recovery of cyber incidents, addressing both internal systems and external stakeholder interactions, and incorporating key performance metrics such as Mean Time to Detect (MTTD), Mean Time to Respond/Recover (MTTR), Recovery Point Objective (RPO), and Recovery Time Objective (RTO). The effectiveness of the CCMP shall be tested at least once every year through mock drills and cybersecurity exercises to ensure preparedness and continuous improvement.	**Chapter VII and Chapter III**	**Relaxed (Within One Year)**
		Cyber Security Audit	**Required Documents:** Cyber Security Audit Report, Compliance Closure Report/Compliance closure certificates, Audit Observation Tracker. To be conducted once in every financial year, with a minimum interval of nine (9) months and a maximum interval of fifteen (15) months between two consecutive audits. No more than three (3) consecutive audits shall be conducted by the same auditing agency or personnel. Cyber Security Audit should be conducted within one year from the date of plant commissioning. During checklist verification, valid documentary evidence of certification progress/completion shall be reviewed. A formal undertaking confirming compliance with the requirement shall be submitted and duly signed by the CISO.	**Chapter IX and Chapter III**	**Relaxed (Within One Year)**

		VAPT	**Required Documents:** VAPT Policy, Vulnerability Assessment Report, Penetration Testing Report, Vulnerability Closure Report, Risk rating, Retesting reports, Final VAPT Report (Pre-Go-Live) **Vulnerability Assessment (VA) -** A structured vulnerability management program shall be implemented for IT and OT systems, including Periodic vulnerability assessment of all IT and OT assets Timely remediation and patch management, with risk-based prioritization and documented closure of identified vulnerabilities. **Penetration Testing (PT)** – The scope for the PT comprises all IT Infrastructure and Lateral Movement from IT to OT. All VAPT findings shall be documented, tracked to closure, and reports shall be reviewed and approved by the CISO.	**Chapter - III**	**Mandatory (Immediate)**
5	**Operations & Maintenance Security Practices**	**Vendor Cybersecurity Requirements (Closure based on inspection visit)**	**Required Documents:** Provide Software and Hardware Bill of Materials (SBOM) as per CERT-In guidelines. O&M sign-off, Vendor list for IoT devices, Vendor Risk Assessment Reports, All OT equipment deployed for control and operation of power system shall be complied with relevant testing standards as well as orders issued by the Government of India, OEM Security Compliance Declaration	**Chapter VIII**	**Mandatory (Immediate)**
		Remote Access Control (Closure based on inspection visit)	**Required Documents:** Reports approved by CISO **Points for Verification:** Physical isolation of OT systems from internet and IT systems (with controlled exceptions), Remote operation (if required - must be with secure, approved, isolated channels), Whitelisted and dedicated applications especially for OT systems, Time-bound access(Just In Time), Session recording, Activity logging, Access approval workflow documented, Role based access control configured, No shared credentials, Process for vendor exit, MFA for critical systems	**Chapter - III**	**Mandatory (Immediate)**
		Backup of Critical Systems (Closure based on inspection visit)	**Required Documents:** Reports approved by CISO **Points for Verification:** Maintain online + offline backups(minimun 180 days), Stored in separate, safe, secure environment, Share details of all new/replaced critical systems to CSIRT-Power Timeline: within 30 days	**Chapter - III**	**Mandatory (Immediate)**
		Data Security & Localization (Closure based on inspection visit)	**Required Documents:** Reports approved by CISO **Points for Verification:** Offline backups of sensitive data must be taken minimum 180 days, Sensitive data must be Encrypted, Secure, Stored within India	**Chapter - III**	**Mandatory (Immediate)**
		Asset Register Maintenance (Closure based on inspection visit)	**Required Documents:** Reports approved by CISO **Points for Verification:** All cyber assets (hardware, software, ownership, patches), All critical systems: Configuratio, Network architecture, Data flow Should be maintained	**Chapter - III**	**Mandatory (Immediate)**
		Time Synchronization (Closure based on inspection visit)	**Required Documents:** Reports approved by CISO **Points for Verification:** All IT/OT systems must use synchronized clocks, Based on reference time source (after risk assessment)	**Chapter - III**	**Mandatory (Immediate)**
		Monitor IT & OT systems continuously and Log Management (Closure based on inspection visit)	**Required Documents:** Reports approved by CISO **Points for Verification:** 24×7 monitoring, Logs should be maintained, Logs sources, Log architecture diagram, sample logs from each source, 180-day retention policy	**Chapter - III**	**Mandatory (Immediate)**
		Cyber Awareness & Training	**Required Document**s: Reports approved by CISO **Points for Verification:** UnderTaking to by signed by CISO 1. Training Records; 2. OT operator awareness, training 3. Awareness Program Reports 4. Mock Drills & Security Exercises It shall be a continuous and ongoing process, conducted at least once in every six months	**Chapter - III**	**Relaxed (Within 6 Months)**
Note: All Concerned Documents should be submitted and will be verified during the inspection visit. Verification Part of Physical Visit Activities and Can be Verify though Annexure-A. Intimation for the physical visit should be initiated atleast before one month from the FTC.					

S. No	Control Area	Description	Required Document	Verification Method	Required before Go Live(Must Have/Should Have(In Some Time Window)/Good to Have
1	**Network Segmentation & Architecture**	Firewall configuration and Network Architecture,Network Segmentation Details	1. Zone diagram, asset-to-zone mapping table, OT-IT isolation evidence, OT-IT Communication Medium	Physical Visit at Site and Document Signed by CISO	Must Have
2			2. Network diagram, DMZ host list, data flow diagram	Physical Visit at Site and Document Signed by CISO	Must Have
3			3. Firewall rule export, rule review, sign-off, default-deny evidence, Firewall Policy	Physical Visit at Site and Document Signed by CISO	Must Have
4			4. Minimum Basic Technologies Defined in Network Architecture(Firewall, Public Facing Applications, OT DMZ Design, DNS Resolution, Internal Network Flow from Firewall)	Physical Visit at Site and Document Signed by CISO	Must Have
5			5. Packet filtering & Deep Packet Inspection (DPI), Content, user & application-based filtering, Encrypted traffic inspection, Geo-fencing, Automatic signature & behavior updates, APIs Security, Web Application Firewall (WAF), Endpoint Detection & Response (EDR/XDR)	Physical Visit at Site and Document Signed by CISO	Should Have (Within 1 year)
6			6. SRA/VPN config, MFA policy, access approval log, session recording config, Access Controls Methods	Physical Visit at Site and Document Signed by CISO	Must Have
7	**Access Control & Identity Management**	Access Control for All IT-OT Systems that have IP Address	1. User account list, role-permission matrix, Role based Access Control config screenshots for all systems 2. All default usernames/passwords changed for all systems 3. Password policy implemented 4. All unused ports/services disabled 5. Latest patches applied on all systems 6. USB access controlled/restricted 7. Policy for Admin Access 8. Access control policy 9. A dedicated physical kiosk scanning station or a formal transient/portable media sanitization procedure before any device enter into the plant.	Physical Visit at Site and Document Signed by CISO	Must Have
8	**SCADA/DCS Security**	Secure access to SCADA Systems	1. Digital Data Protection and Privacy Policy approved. 2. Encryption-at-rest on OT servers and removable media. 3. Encryption-in-transit for SCADA WAN links confirmed. 4. Access Controls for SCADA/DCS 5. SCADA/PLC System Process Flow Diagram	Physical Visit at Site and Document Signed by CISO	Must Have
9	**Physical Security and Server/Control Room Access**	Secure access to Server/Contol Room	Register logs Maintained User Access Logs screenshot Access Method Defined	Physical Visit at Site and Document Signed by CISO	Must Have

10	**Monitoring, Detection & Incident Response**	Monitoring of All IT-OT Sytems	1. SIEM deployment report, OT log integration evidence, alert use-case list, Network Devices Integrated with SIEM, Logs Sources Defined 2. NTP topology diagram, config screenshots, log timestamp validation. Log timestamps aligned end-to-end. 3. Logs receiving from All IP based system, Logs monitoring, incident reporting process 4. Details of IoT/ Smart devices with their input and output data flow connections and protocols used 5. Details of grid integration	Physical Visit at Site and Document Signed by CISO	Must Have
11	**Remote Access Security**	Secure Access Should be In Place	1. Physical isolation of OT systems from internet and IT systems (with controlled exceptions) 2. Remote operation (if required) must be with secure, approved, isolated channels. Whitelisted and dedicated applications especially for OT systems 3. Time-bound access(Just In Time) Session recording, Activity logging, Access approval workflow documented. 4 Role based access control configured 5.Process for vendor exit 6. MFA for critical systems	Physical Visit at Site and Document Signed by CISO	Must Have
12	**Backup, Recovery & OT Resilience**	Backup of The Systems	1. Backup schedule, storage location, ransomware-protection evidence, document access policy 2. Stored in separate, safe, secure environment	Physical Visit at Site and Document Signed by CISO	Must Have
13	**System Hardening & Configuration Mgmt**	Solutions Deployment, OS Hardening & OT System Hardening Mechanism, Configuration Management	All IT and OT systems should be hardened enough to safeguard against malware and cyber threats.	Physical Visit at Site and Document Signed by CISO	Must Have
14	**Asset Visibility & Inventory Management**		1. All IT assets (hardware, software, ownership, patches, OEM Details) 2. All critical systems list maintained	Physical Visit at Site and Document Signed by CISO	Must Have
15	**Vendor Verification**	Vendor and Related OEM Details	1. Vendor list for IoT devices 2. Vendor Risk Assessment Reports 3. All OT equipment deployed for control and operation of power system shall be complied with relevant testing standards as well as orders issued by the Government of India 4.OEM Security Compliance Declaration 5. Provide end-of-life (EOL) / end-of-support details for hardware/software. 6. Provide Software Bill of Materials (SBOM) as per CERT-In guidelines. 7. O&M sign-off 8. Third-party open-source vulnerability scanning before onboarding software components into the OT network.	Physical Visit at Site and Document Signed by CISO	Must Have