WHITEPAPER

SHIELDWORKZ

The CEA (Cyber Security in Power Sector) Regulations, 2026

A Comprehensive Compliance Analysis and the Shieldworkz Path to $5M Revenue

Shieldworkz OT Systems | August 2026 |
SWZ-REF-REG-202608-001 Rev C

ASSET INVENTORY | RISK ASSESSMENT | NETWORK SECURITY | THREAT DETECTION | VULNERABILITY MANAGEMENT | COMPLIANCE REPORTING

1. Executive Summary

On 31 July 2026 the Central Electricity Authority notified the CEA (Cyber Security in Power Sector) Regulations, 2026 in the Gazette of India (Extraordinary, No. 484, Part III, Section 4; e-gazette publication 5 August 2026). Issued under Section 177(1) read with Section 73(c) of the Electricity Act, 2003, with MeitY concurrence, the regulations convert India's power-sector cybersecurity framework from the 2021 guidelines regime into a binding, audited, evidence-based compliance mandate. Enforcement begins 1 April 2027; six dependency-heavy provisions are deferred to separate CEA orders.

Approximately 1,000-1,500 entities are directly regulated - generators at or above 50 MW, all transmission and distribution licensees, all load despatch centres, and power exchanges - with vendors directly bound for the first time. The serviceable core with real OT estates and standalone budgets is roughly 200-300 entities. The regime demands 18+ maintained documents and registers, annual third-party audits with auditor rotation, six-hour incident reporting, hard data localization, and OT air-gap defaults. Most covered entities lack a compliant CISO organisation; none possess the mandated document suite; no vendor offers an integrated compliance platform for this regulation.

This paper provides a chapter-by-chapter analysis of the regulations, a complete deliverables inventory, market sizing, a prioritised account list, the OThello Assess product fitment, and a concrete revenue model showing how Shieldworkz reaches $5M in CEA-2026-driven revenue across FY2027-28 through six service lines at realistic Indian price points and penetration rates.

2. Regulatory Background and Timeline

India's power-sector cybersecurity journey: the CEA Cyber Security Guidelines of October 2021 introduced CISO appointment, ISO 27001 alignment and sectoral CERT reporting as guidance; the Ministry of Power stood up six sectoral CERTs (thermal, hydro, transmission, grid operation, renewable energy, distribution); draft regulations circulated in 2024 and again in October 2025 for public comment. The 2026 notification is the culmination - guidance becomes law.

Milestone	Date
CEA Cyber Security Guidelines (non-binding)	October 2021
Draft CEA Cyber Security Regulations published for comment	7 October 2025
Final regulations notified, Gazette of India No. 484	31 July 2026
E-gazette publication (CG-DL-E-05082026-275218)	5 August 2026
All non-deferred provisions in force	1 April 2027

Milestone	Date
Deferred provisions 5(9), 5(24), 5(33), 5(39), 6(2), 6(7)	Separate CEA orders with prior Central Government approval

3. Scope, Applicability and Key Definitions

3.1 Covered Entities (Reg 2, Reg 3(w))

The regulations apply to every entity that owns, operates or manages Operational Technology infrastructure associated with the interconnected power system, together with IT infrastructure physically or logically connected to that OT - existing and upcoming. The defined term includes:

- Generating companies, captive generating plants and Energy Storage System organisations - these three categories alone carry the 50 MW installed-capacity threshold; entities below 50 MW are only encouraged to adopt CERT-In's "15 Elemental Cyber Defense Controls for MSMEs"
- Transmission licensees - CTU, state transcos and private TBCB licensees, with no capacity threshold
- Distribution licensees - state, private and deemed licensees, no threshold
- National, Regional and State Load Despatch Centres
- Power exchanges and over-the-counter platforms - exempt only from Regs 6 (OT), 11 and 12 (vendor chapters)

Vendors are directly bound by Regs 11-12: OEMs, original equipment suppliers, system integrators, hardware/software suppliers, contractors and service providers including cloud service providers - and, through Reg 12, every manufacturer and supplier of inverters, communication modules, monitoring systems and energy-management software for prosumer-owned Distributed Generation Resources (generation feeding in below 33 kV, including rooftop solar and ESS). Prosumers themselves are not regulated; their vendors are.

3.2 Definitions That Shape Scope (Reg 3)

Term	Practical Effect
Critical system	Critical OT system, critical IT system, or both - anything whose unavailability or degradation adversely impacts business operations; includes CII where applicable. Most obligations attach to this class
Cyber asset	Any programmable electronic device connected over a network, with or without computing capability, including hardware, software, sub-components and data - sweeps in RTUs, IEDs, relays, meters
Electronic Security Perimeter	The logical border around IT/OT systems within which access is monitored and controlled - the anchor for perimeter-device obligations
Remote access vs remote operation	Access = any reach into a cyber asset via external network; operation = day-to-day running from a distant location. Separately regulated: access is exception-only; operation requires board approval and must stay within India
Trusted source	The mechanism for supply-chain vetting per Central Government criteria - the hook for the deferred procurement clauses, aimed squarely at Chinese-origin equipment
Cyber sabotage	Deliberate malicious disruption/damage/destruction - triggers the accelerated 24-hour reporting class

4. CSIRT-Power: The New Sector Regulator-Operator (Chapter II)

The Computer Security Incident Response Team - Power is established by the Ministry of Power as an extended arm of CERT-In. Its directions are binding on entities and vendors (Reg 4(3)). Its mandate:

- Coordinating agency for reporting and responding to power-sector cyber incidents; nodal agency for analysis, prediction and prevention
- Power to collect from any entity: network architecture, asset details, logs, forensic records and images, policies and procedures - in the form and manner it specifies (sensitive data restricted to designated government agencies; no third-party disclosure without explicit communication to the entity)
- Issues alerts, advisories, guidelines and threat intelligence jointly with CERT-In and NCIIPC
- Creates SOPs, sub-sector benchmarks, security controls and incident-response best practice in consultation with regulators and entities
- Drives sector posture through assessments, audits, certification audits, self-audits, third-party audits, mock drills and simulations
- Advises entities on Cyber Crisis Management Plans and coordinates their execution during actual crises
- Formulates supply-chain security measures for specified cyber assets; facilitates R&D; with industry and academia
- Central and regional cyber security coordination forums to be established by separate CEA order; sub-sectoral CSIRTs may be designated for generation, transmission, distribution and grid operation

5. General Cyber Security Requirements - Regulation 5 (All Entities)

Regulation 5's forty-two clauses are the compliance core. Grouped thematically:

5.1 Governance and the CISO Organisation (5(1)-(10))

- Designate regular senior-management employees as CISO and alternate CISO; positions never simultaneously vacant; roles defined per Central Government framework; CISO reports to the head of the entity (for SLDCs within holding companies, a separate CISO reporting to the holding-company head)
- Minimum three-year CISO tenure; role ring-fenced to cyber security matters only; contact details published and communicated to CSIRT-Power and all stakeholders; at least five man-days of cyber security training per financial year
- Dedicated Information Security Division in India, headed by the CISO, operational 24x7, sufficiently staffed, with certified staff on three-year minimum postings and five man-days annual power-sector training [DEFERRED - 5(9)]
- Defined, documented Cyber Security Policy approved and reviewed annually by the head or board

5.2 Crisis Management and Architecture (5(11)-(17))

- Cyber Crisis Management Plan prepared in consultation with CSIRT-Power, vetted by CERT-In, approved and reviewed annually by head/board

- IT networks containing Critical Information Infrastructure separated from the internet and from other IT networks; where internet is unavoidable, sourced securely with hardening per designated-agency specification
- Electronic Security Perimeter equipped with firewalls and devices delivering packet filtering, deep packet inspection, content/user/application filtering, encrypted-traffic detection and inspection, intrusion detection and prevention, geo-fencing, automatic and user-controlled signature/behaviour updates, and anomaly-based detection
- Public-facing web services, portals and APIs deployed only after cyber security audit clearance; updates tested, confirmed vulnerability-free, and audit-cleared where policy-qualified; non-qualified updates assessed at the next audit
- Security devices for all critical web applications with application-layer filtering and bidirectional protection
- Systems identified and segregated as critical and non-critical per documented policy procedure
- Remote access to cyber assets exception-only (troubleshooting and emergencies): non-critical assets with CISO approval and controls; critical systems only after comprehensive risk assessment, with continuous monitoring; risk-assessment records, physical approval documents and logs retained per data-retention policy

5.3 Data, Vendors and Assurance (5(18)-(31))

- Awareness programmes and exercises including mock drills and tabletops at least every six months
- Sensitive information and data - including cloud-hosted and historical - stored encrypted, secured, and residing within India only
- All cyber security requirements, applicable rules and an NDA embedded in vendor SLAs, surviving contract expiry; vendor personnel touching critical systems admitted only after personnel risk assessment, mitigation and an SLA-compliance undertaking; breach triggers mandatory enquiry and action against the vendor including cloud providers
- Online and offline backups of all critical systems in a separate, safe, secure environment
- Comprehensive annual cyber security audit of all critical systems: 9-15 months between audits; auditing agency deploys qualified personnel excluding any staff seconded to the entity; no three consecutive audits by the same agency or personnel
- All IT products procured in compliance with, and tested against, Central Government orders
- ISO/IEC 27001 or Technical Criteria Certificate covering all critical systems; no four consecutive certification audits by the same agency/personnel [DEFERRED - 5(24)]
- Asset registers: (a) all cyber assets with ownership, hardware, firmware, software and patch detail; (b) all critical systems with configuration, hardware, software, network architecture depicting data flows, and communication protocols - reviewed annually or on any commissioning/replacement, whichever is earlier
- Cyber Risk Assessment and Mitigation Plan for every registered asset: updated six-monthly, reviewed annually, implemented
- Pre-commissioning cyber security audit including vulnerability assessment and penetration testing for every new or replaced critical system
- System details of new/replaced critical systems furnished to CSIRT-Power within 30 days
- Relevant information to NCIIPC for CII identification; within 60 days of CII identification, approach the Appropriate Government for Protected System notification

- CII and Protected Systems not discoverable on public platforms absent head/board approval on documented business grounds
- Procurement mandates Factory Acceptance Testing and Site Acceptance Testing including cyber security requirements

5.4 Operations Hygiene (5(32)-(42))

- Clock synchronisation of all relevant processing systems to a policy-defined reference time source, preceded by detailed cyber risk assessment
- All personnel - including vendor O&M; staff on critical systems - complete designated power-sector cyber security courses [DEFERRED - 5(33)]
- Physical-security systems, networks and applications physically separated from critical-system networks (logically, with head approval, where physical separation is infeasible)
- Incident Response and Recovery Plan maintained, reviewed and updated at least six-monthly
- Surveillance and continuous monitoring of IT and OT systems for threats and vulnerabilities, with incident response and remediation support
- Logging enabled on all ESP security devices; perimeter rules and policies reviewed at least annually
- IT equipment and services from trusted sources per Central Government orders [DEFERRED - 5(39)]
- Compliance with the IT Act 2000 and all subordinate rules, in addition to these regulations
- Structured vulnerability disclosure and management programmes with vendors and CSIRT-Power
- Incident register maintained in CSIRT-Power's prescribed format

6. Additional OT Requirements - Regulation 6

- 6(1) Physical isolation of OT from the internet and from IT as the default. IT/OT interconnection only where business requires, per policy procedure, with hardened logical separation, risk assessment, head/board approval, continuous monitoring for malicious activity, and retention of approvals and logs
- 6(2) Perimeter cyber security devices including firewalls at every OT interconnection point with the power system's communication network: OT-protocol-aware detection and filtering, content/user/application filtering, deep packet inspection, intrusion detection, geo-fencing, anomaly-based detection - with signature updates performed offline only [DEFERRED]
- 6(3) Control and operation of power-system elements, and exchange of information including real-time data, over dedicated internet-isolated channels through perimeter devices, confined to national boundaries. Cross-border entities: only via dedicated separate communication systems and unidirectional gateways, continuously monitored. End-consumer real-time data: secured connections isolated from public access, sensitive exchange encrypted
- 6(4) Remote operation, where business-necessary, only within India, with prior head/board approval, over a dedicated internet-isolated channel carrying the 6(3) security stack
- 6(5) All OT equipment, components and parts for power-system control/operation compliant with Central Government orders
- 6(6) OT communication systems isolated from IT communication systems
- 6(7) OT equipment and services from trusted sources per Central Government orders [DEFERRED]
- 6(8) OT environment segmented into trust levels by criticality, security requirements and risk assessment
- 6(9) Inter-entity OT data channels protected by the owner of the communication system

7. The CISO and Information Security Division - Regulation 7

Qualifications: Indian citizen and resident; engineering degree or equivalent from a recognised institute; at least fifteen years' experience in the power sector or IT. The Authority may specify additional qualifications by separate order. The alternate CISO discharges the role in the CISO's absence.

Functions (with ISD assistance) include:

- Incident reporting to CSIRT-Power and CERT-In within six hours; concluded cyber sabotage in critical systems within twenty-four hours
- Quarterly review of policy-mandated compliances; implementation of control measures for critical systems and, for CII/Protected Systems, NCIIPC-validated controls
- Acting on directives from the Central Government, CEA, CERT-In and CSIRT-Power
- Threat-intelligence gathering, analysis, threat-vector identification, risk assessment and mitigation
- Detailed incident reports, action-taken reports and root-cause analyses shared with CSIRT-Power and CERT-In
- Custody of all First Schedule documents; retention of all cyber data per the data-retention policy
- Firmware/software patching of critical systems per policy; log and forensic-record storage assurance
- Public-IP inventory (allocated, used, unused) to CSIRT-Power

- Random testing of critical-system day-to-day operations for policy conformance, with corrective measures
- Procedures for remote access (non-critical), secure OT remote operation, and time-source synchronisation; development and upkeep of the CSP, CCMP, data-retention and backup policies; asset-register and risk-plan preparation and review

8. The Cyber Security Policy - Regulation 8 (33 Mandated Elements)

The CSP must align with the entity's Business Continuity Plan across IT and OT. Its thirty-three elements, grouped:

Group	Elements
Foundations (1-4)	Purpose and scope with all applicable requirements; NCIIPC alignment for Protected Systems; stakeholder roles; cyber-asset register procedure with criticality/risk classification
Criticality & risk (5-8)	System identification and critical-system classification by BCP impact (annual review); risk assessment and mitigation procedure per asset (annual review); vulnerability/threat management mechanism for critical systems; cyber-sabotage identification and reporting procedure
Response & testing (9-10)	Incident Response & Recovery Plan with incident taxonomy, risk analysis and incident-specific response plans - incidents needing entity-level strategic recovery are classified as crises; random-testing mechanism that must not disrupt operations or safety
Access & personnel (11-13)	AAA-based access management for critical systems, public applications and sensitive data; personnel risk assessment for vendor-deployed staff including on role change and post-termination/resignation/superannuation; physical access-point security with continuous monitoring and revocation on perceptible threat
Supply chain & remote (14-16)	Cyber supply-chain risk management for critical systems and services; remote-access procedure with least privilege, minimum duration, MFA and geo-fencing; remote-operation procedure reviewed annually or on business change
Data (17-19)	Digital data protection and privacy policy per Central Government rules; backup policy - data no older than one month, integrity and restoration tested against BCP (annual review); encryption of sensitive data at rest, in backup and in transit (unencrypted transmission only over dedicated channels where encryption infeasible)
People & lifecycle (20-23)	Annual training for all personnel with critical-system access; internet access policy; obsolete-asset phase-out and secure disposal; R&D; collaboration plan gated by risk assessment and NDA
Change management (24-25)	Two-category update classification - prior-audit-required vs next-audit-assessed (suggestive Second Schedule list revisable by CSIRT-Power with CEA approval); change-management process with version control and rollback; OT patches digitally signed by OEM, risk-assessed, tested in simulated environments, deployed offline; unsigned patches verified for validity and authenticity
Records & flows (26-33)	Log/forensic storage mechanism; reference time source terrestrial or India-specific satellite, internet-independent for OT; IT-OT logical separation with data flowing via separate channels and unidirectional gateways; cross-border data classification procedure (reviewable by CSIRT-Power); critical web-application classification; secure disposal of obsolete assets and of sensitive data; the data-retention policy itself

Data-retention floors specified within element 33: last two working backups always available; remote-access risk assessments, approvals and logs one year; FAT/SAT reports for the asset's life; remote-operation records one year; cyber security audit reports three years; certification audit reports four years; self-audit reports three years; all ICT and IT-OT interconnection logs and forensic records 180 days; incident-associated logs (spanning 180 days before and after) retained at least 365 days from occurrence. Access to retained records restricted to authorised persons; the Authority may extend the list by separate order.

9. Cyber Crisis Management Plan - Regulations 9-10

- The CCMP must contain: detailed SOPs to detect and identify all incidents; criteria for classifying an incident as a crisis; the list of all possible crisis scenarios; stakeholder identification with roles, responsibilities and their communication; the manner and mode of internal/external coordination during crisis; and mitigation measures for fastest recovery
- Entity responsibilities: ensure availability of all essential communications during crisis; test CCMP efficacy at least annually through exercises and mock drills on scenarios selected for that year - selections must not repeat previously tested scenarios until the full cycle completes
- After every actual crisis: a detailed report covering handling, recovery, experience, lessons, feedback, lapses and proposed measures; relevant information shared with CSIRT-Power and stakeholders; the CCMP updated with qualified observations

10. Vendor Obligations - Regulations 11-12

10.1 All Vendors (Reg 11)

- Documented, tested restoration procedures and recovery plans for supplied systems
- Digitally signed or validated security patches and updates for all supplied systems and components, available through the contract period or the system's useful life, whichever is later
- Detailed integration documentation, including third-party component patch/update requirements
- End-of-support / end-of-life disclosure for all supplied software, hardware and systems, including third-party sourced
- Bill of Materials per CERT-In guidelines: a detailed list of all components, including firmware, deployed in critical systems
- Hardware and software hardened - all inherent security capabilities, secure configuration and controls enabled - before supply
- A formal structured vulnerability-reporting process for entities; vulnerabilities furnished to CSIRT-Power through the vendor's own disclosure and management programme

10.2 Prosumer DGR Vendors (Reg 12)

- Applications, monitoring/control servers and real-time data - including cloud-hosted and historical - stored encrypted and residing exclusively within India
- Remote access/operation of grid-connected devices, and real-time data exchange with remote applications, aggregators and distribution licensees, only over secure channels after mutual authentication, with encrypted communication
- Information for trusted-source verification per Central Government orders; commencement for existing DGR fleets to be specified by separate CEA order

Practical effect: the entire smart-inverter ecosystem serving Indian rooftop solar - dozens of brands, heavily Chinese-origin - now carries direct Indian regulatory obligations on data residency, secure remote access and supply-chain verification.

11. The Audit Regime - Regulations 13-15

Who may audit: Reg 3(p) defines a cyber security audit as one conducted by a CERT-In empanelled auditor, or any other auditor designated by the Ministry of Power through separate order. The empanelment requirement therefore attaches to every statutory audit - annual (5(22)), pre-commissioning including VAPT (5(27)), and web-application clearance (5(14)). Self-audits (Reg 15) are conducted by the entity itself; ISO 27001/TCC certification (5(24)) requires an accredited certification body, a separate track. The MoP-designation clause leaves a second door open for a future power-sector-specific auditor panel.

- Audit scope per CSIRT-Power guidelines and designated-agency directions; every audit verifies closure of all previous audit findings
- Auditor's report due within six weeks of audit commencement; critical and high-risk vulnerabilities remediated within one month of report submission; medium and low within three months; compensatory controls deployed for critical/high items until audit clearance
- CISO reviews audit compliances and ensures the auditor's closure report lands within six months of audit commencement; major findings and critical-system non-compliances reported to the head or board
- CISO-Ministry of Power may demand any entity's audit closure report at any time; after written clarification, with CEA approval and notice, may appoint a third-party auditor at the entity's cost; divergent third-party findings trigger further action
- Annual self-audit against all applicable regulations; a board or senior-management member may be designated accountable; non-compliances remediated before the next financial year's self-audit; CISO-MoP may verify self-audit claims via third-party audit at the entity's cost

12. Enforcement and Penalties - Regulations 16-17 and Parent Statutes

Mechanism	Exposure
Electricity Act 2003, s.142 (via petition by CISO-MoP to the Appropriate Commission)	Up to Rs. 1 lakh per contravention plus Rs. 6,000 per day continuing. Modest sums - but a s.142 finding reaches licence conditions, tariff proceedings and lender covenants
IT Act 2000, s.70 - Protected Systems (the destination of the Reg 5(29) NCIIPC route)	Unauthorised access to a Protected System: criminal offence, up to ten years' imprisonment plus fine
IT Act 2000, s.70B(7) - non-compliance with CERT-In directions (CSIRT-Power is its extended arm; directions binding under Reg 4(3))	Up to one year imprisonment or Rs. 1 lakh fine or both
IT Act 2000, s.43A / s.45	Compensation and residual penalties for data-protection failures
Third-party verification audits (Regs 14-15)	Appointed by CISO-MoP; cost borne by the entity regardless of outcome
Soft enforcement	MoP performance reviews and RDSS funding conditionality for public utilities; s.19 licence-revocation exposure behind persistent non-compliance; cyber-audit status in lender due diligence on TBCB and RE project finance

Reg 17 preserves a relaxation power: the Authority may, in writing, relax any provision on its own motion or on application, to remove hardship for a class of persons. Direct monetary penalties are weak

by global standards (contrast NIS2's 2% of turnover or NERC CIP's $1M per day per violation); the real teeth are criminal Protected System liability, binding CSIRT-Power directions, and regulatory and financing leverage.

13. The Six Deferred Provisions

Provision	Requirement	Dependency
5(9)	24x7 India-based Information Security Division under the CISO: sufficient certified staff, five man-days annual training, three-year postings	Largest cost and manpower item; sector-wide certified 24x7 capability unachievable by April 2027
5(24)	ISO/IEC 27001 or Technical Criteria Certificate for all critical systems, with four-audit rotation	Certification capacity and cost across 1,000+ entities
5(33)	Designated power-sector cyber courses for all personnel including vendor O&M; staff	The designated courses must first exist
5(39)	Trusted-source procurement - IT equipment and services	Awaits the trusted-source verification mechanism being operationalised
6(2)	OT-protocol-aware perimeter devices at every OT interconnection point; offline-only signature updates	A hardware procurement cycle most discoms have not budgeted
6(7)	Trusted-source procurement - OT equipment and services	Same mechanism dependency as 5(39)

Everything else is enforceable 1 April 2027. Each deferred-provision order, when issued, is a discrete demand trigger - most notably 6(2) (perimeter hardware) and the trusted-source pair (supply-chain displacement of Chinese-origin inverter and SCADA stacks).

14. Complete Compliance Deliverables Inventory

Thirty-six deliverables across six categories. The First Schedule places twelve in the CISO's formal custody: the CSP with its documents and procedures, CCMP, data-retention policy and its records, ISO/TCC certificate, asset registers, risk assessment and mitigation plan, IR&R; plan, incident register, bill of materials, BCP, and the remote operation and remote access procedures.

14.1 Governance documents (board/head-approved)

#	Deliverable	Cadence
1	Cyber Security Policy (33 elements, Reg 8)	Annual head/board review
2	Cyber Crisis Management Plan (CSIRT-Power consulted, CERT-In vetted)	Annual approval; annual scenario testing, non-repeating
3	Business Continuity Plan	CSP alignment anchor
4	Data Retention Policy	Annual review
5	Backup Policy	Annual review; backups no older than 1 month; restoration tested
6	Digital data protection & privacy policy	Per Central Government rules
7	Internet access policy	Defined, authorised use only

14.2 Registers

#	Deliverable	Cadence
8	Cyber asset register (ownership, hardware, firmware, software, patch)	Annual or on commissioning

#	Deliverable	Cadence
9	Critical systems register (config, architecture, data flows, protocols)	Annual or on commissioning
10	Cyber security incident register	CSIRT-Power format, continuous

14.3 Plans, assessments and processes

#	Deliverable	Cadence
11	Cyber Risk Assessment & Mitigation Plan	6-month update; annual review
12	Incident Response & Recovery Plan	6-month review
13	Personnel risk assessments (vendor staff; incl. post-exit)	Role-based; on change
14	Remote access procedure + per-access risk record, approval, logs	Records kept 1 year
15	Remote operation procedure	Annual review; records 1 year
16	Obsolete-asset phase-out and secure disposal procedures	Incl. sensitive-data disposal
17	Supply-chain risk management process	Critical systems and services
18	Change management process (version control, rollback, OEM-signed OT patches, simulated testing, offline deployment)	Continuous

14.4 Certifications and audit artifacts

#	Deliverable	Retention / timing
19	ISO/IEC 27001 or Technical Criteria Certificate	Deferred commencement
20	Annual cyber security audit report + closure report	Report 6 weeks; closure 6 months; retain 3 years
21	Certification audit reports	Retain 4 years
22	Annual self-audit report	Retain 3 years
23	FAT/SAT reports incl. cyber testing	Asset life
24	Pre-commissioning VAPT reports	Every new/replaced critical system

14.5 External filings and notifications

#	Deliverable	Deadline
25	CISO/alternate CISO details - public + CSIRT-Power	Kept current
26	New critical-system details to CSIRT-Power	30 days
27	CII information to NCIIPC; Protected System approach	60 days from identification
28	Incident reports, ATRs, root-cause analyses	6 hours; 24 hours for sabotage
29	Public IP inventory to CSIRT-Power	As required
30	Crisis handling and lessons-learned reports	After each actual crisis

14.6 Vendor-side deliverables (contractually demanded)

#	Deliverable	Basis
31	SBOM per CERT-In guidelines	Reg 11(5)

#	Deliverable	Basis
32	Tested recovery procedures for supplied systems	Reg 11(1)
33	Signed patches - contract period or useful life	Reg 11(2)
34	Third-party component integration documentation	Reg 11(3)
35	EOL/EOS declarations	Reg 11(4)
36	Hardened delivery; formal vulnerability reporting; SLA + NDA	Regs 11(6)-(7), 5(20)

15. Market Sizing

15.1 Directly Regulated Entities: ~1,000-1,500

Category	Count	Composition
Grid operators	~40	NLDC, 5 RLDCs, ~33 SLDCs
Transmission licensees	~90-110	CTU/Powergrid + SPVs; 30+ state transcos; 50+ private ISTS TBCB SPVs (each a separate licensee)
Distribution licensees	~75-85	~55-60 state discoms; private/deemed (Tata Power-DDL, BSES x2, Torrent, CESC, Adani Electricity Mumbai, SEZ deemed); JV discoms
Generators >=50 MW	~800-1,200	Thermal/hydro/nuclear a few hundred; RE SPVs the swing factor (per-entity vs per-plant threshold reading); captive >=50 MW adds 150-300; grid-scale ESS ~20-40 and growing
Exchanges/OTC	~5	IEX, PXIL, HPX + OTC platforms

Sub-50 MW generators and prosumers fall outside entity scope. The practical addressable core with real OT estates and standalone compliance budgets is ~200-300 entities: discoms, transcos, load despatch centres and large gencos. Most renewable SPVs will comply at group level, compressing 1,000+ nominal entities into perhaps 80-120 buying centres.

15.2 The CISO and Capability Gap

The CISO mandate dates to the 2021 guidelines, so paper designation is high in the government sector: effectively 100% among CPSUs (named CISOs since 2021-22 with real organisations behind most), roughly 70-85% among state utilities and SLDCs (typically a dual-hatted Director-IT or Chief Engineer), and under 30-40% among private IPPs, RE SPVs and industrial captives (group CISOs at Adani, Tata, JSW and ReNew; standalone SPVs mostly uncovered). Estimated 300-500 of the covered entities have a formally designated CISO.

The 2026 regulations expose a quality gap rather than an existence gap. The ring-fencing requirement eliminates the dual-hat model dominating state utilities; the regular-employee, three-year-tenure rule eliminates consultant and deputationist arrangements; the fifteen-year experience bar narrows the candidate pool; and the coming 24x7 ISD implies a real headcount commitment (the 2024 draft contemplated a minimum of four officers plus four shift staff). India does not have 1,000+ qualified power-sector CISOs available. Even entities that "have a CISO" face re-appointment and ISD build-out before April 2027 - the structural driver behind virtual-CISO, ISD-design and managed-SOC demand.

16. Target Accounts

Tier 1 - Anchors (large OT estates, central procurement, reference value)

Account	Rationale
NTPC (+ NTPC Green)	Largest genco, ~70+ GW across dozens of plants
Powergrid	CTU; the country's largest transmission OT estate; NCIIPC-notified systems already
NHPC, SJVN, THDC	Hydro portfolios; remote, RTU-heavy sites
NPCIL	Highest bar, longest cycle - flagship credibility

Account	Rationale
Grid-India (POSOCO)	NLDC + 5 RLDCs; the SCADA/EMS nerve centre - small entity, outsized strategic value
Adani Power / Adani Energy Solutions	Private generation + transmission under one group decision
Tata Power	Generation, transmission and Mumbai/Delhi/Odisha distribution - one group, four entity types
JSW Energy, Torrent Power, CESC/RPSG	Integrated private utilities

Tier 2 - State-sector volume (the bulk of the 200-300 core)

Segment	Accounts
State gencos	MAHAGENCO, UPRVUNL, TANGEDCO, WBPDCL, GSECL, RVUNL, KPCL, TSGENCO, APGENCO, DVC
State transcos	MSETCL, TANTRANSCO, GETCO, RVPN, UPPTCL, TSTRANSCO
SLDCs	30+ entities with identical requirements - a repeatable compliance-in-a-box play (CISO advisory, policy/CCMP drafting, audit preparation)
RDSS-funded discoms	MSEDCL, TNEB/TANGEDCO discoms, BESCOM, UPPCL discoms, PSPCL, WBSEDCL - RDSS funding can carry cyber line items

Tier 3 - High-growth private (fast cycles, greenfield OT, no incumbents)

Segment	Accounts
RE IPPs >=50 MW	Adani Green, ReNew, Greenko, Tata Power Renewables, Sembcorp, Ayana, Avaada, Juniper Green, ACME - SCADA-per-park, group-level compliance buying, minimal OT security today
ESS operators	Greenko pumped hydro, JSW Neo, IndiGrid BESS SPVs - new asset class, no incumbent vendor
TBCB platforms	IndiGrid, Sterlite/GIC, ReNew Transmission - portfolio deals covering many licensees at once
Captive >=50 MW	JSW Steel, Vedanta/BALCO, Hindalco, UltraTech, Reliance refining CPPs - already reachable via IEC 62443 conversations

Tier 4 - Exchanges

IEX, PXIL, HPX: IT-only scope (Reg 6 exempt); fits SOC and audit services rather than the detection platform.

17. OThello Assess: Product Fitment

OThello Assess today delivers full OT security assessments in sub-24-hour cycles - executive summary, system scope, zone security-level heat maps, severity-ranked gaps, recommended controls and remediation plans, with every finding cited to source documents. Because CEA 2026 is fundamentally a document-production-and-evidence regime, the fit is direct. Six workstreams convert the platform into the one-stop CISO compliance product:

Workstream	Description	Regulatory hook
1. CEA 2026 framework pack	All 42 Reg 5 clauses, 9 Reg 6 clauses, 33 Reg 8 elements and Reg 13 audit scope as a native framework, mapped to the existing IEC 62443 control library (~70% maps cleanly to SR/CR). Output: clause-by-clause posture report with the citation-backed evidence trail self-audits and external audits demand	Regs 5, 6, 8, 13, 15
2. Deliverable auto-generation	Repoint the existing AI generation pipeline (pluggable LLM backend): assessment data in, draft policy suite out - CSP structured to the 33 elements, CCMP structured for CERT-In vetting. Assessment to board-ready policy pack in days. No Indian vendor offers this	Reg 8, Regs 9-10
3. Living registers	Passive device-identification output auto-populates the cyber-asset and critical-system registers (configuration, architecture, data flows, protocols); BCP-impact criticality workflow; review obligations become push-button	Reg 5(25)-(26), 8(4)-(5)
4. Compliance cockpit	Obligation calendar: 6-hour reporting, 30-day filings, 60-day Protected System approach, 6-month updates and drills, 9-15 month audit windows, auditor-rotation tracking, retention clocks. Pre-assembled audit binder. Converts one-time assessment into annual renewal	Regs 5, 13-15
5. Incident workflow	CSIRT-Power-format register; templated 6/24-hour reports feeding ATRs and RCAs; NDR detections flow directly into the register - tethers assessment to the platform	Reg 5(42), 7(3)
6. Supply-chain module	SBOM ingestion, vendor SLA clause checklists, personnel risk records, EOL tracking against the phase-out plan; seeds a future vendor-side SKU	Regs 11-12, 5(20)

Structural moat: air-gapped deployment is already an architectural assumption, matching PSU data-localization instincts; clause-cited evidence generation is precisely what survives a CISO-MoP third-party verification audit; and the NDR platform is the natural answer to the 5(36)/6(1) continuous-monitoring mandates that assessments alone cannot satisfy.

18. The Revenue Plan: $5M from CEA 2026

18.1 Six Revenue Lines

Line	Offering	Price Band (USD)	Buyer
R1	CEA gap assessment (OThello Assess CEA Edition): clause-by-clause posture + evidence pack	$12-20K state entities; $25-50K CPSU/large private	All tiers - the universal entry product

Line	Offering	Price Band (USD)	Buyer
R2	Compliance documentation suite: CSP (33 elements), CCMP, IR&R;, retention/backup policies, procedures - AI-generated, consultant-finished	$15-35K per entity; $10K/yr maintenance	Tiers 1-2 first movers; SLDC repeatable pack
R3	Audit preparation and self-audit support subscription: cockpit + evidence packs + finding-closure tracking	$10-20K per year recurring	Every audited entity, annually
R4	vCISO / ISD advisory retainer: qualified-CISO scarcity play; ISD design ahead of 5(9)	$3-6K per month ($36-72K/yr)	State entities and RE platforms without compliant CISOs
R5	Continuous monitoring: NDR platform deployment answering 5(36)/6(1), plus managed SOC as de facto 24x7 ISD capability	Platform $75-250K; managed service $50-150K/yr	Tiers 1-3 with real OT estates
R6	Vendor compliance SKU: Reg 11-12 readiness - SBOM, patch process, hardening evidence, India data-residency architecture	$8-20K per vendor	OEMs, integrators, inverter/EMS suppliers

Statutory audit delivery model: the Reg 3(p) definition requires a CERT-In empanelled auditor for every statutory audit. Shieldworkz operates through an empanelled audit partner - the partner signs the statutory report while Shieldworkz delivers the OT-competent fieldwork, evidence packs and findings via OThello. This adds a seventh revenue line (R7): a share of statutory audit fees on partner-delivered engagements, typically 30-40% of a $15-30K audit fee, while keeping full ownership of the higher-margin preparation and remediation work in R1-R4.

18.2 The $5M Build

Cumulative FY2027-28 (April 2026 - March 2028 selling window against the April 2027 deadline and first audit cycle):

Line	Volume Assumption	Avg Value	Revenue
R1 Assessments	45 entities (15 CPSU/large @ $35K, 30 state/private @ $15K)	$21K blended	$975K
R2 Documentation suites	30 entities (assessment attach rate ~65%)	$25K	$750K
R3 Audit-prep subscriptions	35 entities x avg 1.4 years	$15K/yr	$735K
R4 vCISO retainers	12 retainers x avg 15 months	$4.5K/mo	$810K
R5 Platform + managed SOC	7 platform deals @ $120K + 5 managed contracts @ $90K/yr x 1.5 yrs avg	-	$1,515K
R6 Vendor SKU	8 vendors	$12K	$96K
R7 Statutory audit share (via empanelled partner)	35 partner-delivered audits @ $22K avg fee x 35% share	$7.7K	$270K
		Total	$5.15M

Penetration check: 45 assessed entities is 15-22% of the 200-300 core - aggressive but achievable for a first mover with the only purpose-built product. The 8 platform deals sit inside Tier 1-2 accounts where 5(36)/6(1) monitoring is unavoidable and budgets exist. R3 and R4 are the recurring base that compounds beyond FY28: at steady state, 60 subscriptions plus 15 retainers alone exceed $1.7M ARR before any platform expansion. R7 is deliberately the smallest line: the statutory audit fee is L1-competed commodity work - its value is not the fee share but the account access it creates, since every partner audit seeds an R3 subscription and an R5 monitoring conversation on the findings.

18.3 Quarterly Motion

Window	Focus
Q3 FY26-27 (Oct-Dec 2026)	Framework pack + documentation generation live. Land 8-12 assessments as budget panic starts - state utilities discover the April deadline is real. CERT-In empanelled audit partner signed and co-sell motion live. First 2-3 SLDC wins for CSIRT-Power ecosystem visibility
Q4 FY26-27 (Jan-Mar 2027)	Peak pre-deadline demand: 15+ assessments, documentation attach, first vCISO retainers. Indian fiscal year-end spending (March) - capture unspent state budgets. Cockpit launches for renewal base
Q1-Q2 FY27-28 (Apr-Sep 2027)	Regulations in force; first audit cycle begins (9-15 month windows open). Audit-prep subscriptions convert; platform deals close in Tier 1-2 where audits expose monitoring gaps; managed SOC attaches where 5(9) orders loom
Q3-Q4 FY27-28 (Oct 2027-Mar 2028)	First audit findings drive remediation spend; deferred-provision orders (esp. 6(2), trusted-source) trigger hardware-adjacent and supply-chain work; vendor SKU scales as entities push Reg 11 demands downstream; second fiscal year-end capture

18.4 Execution Requirements and Risks

- Statutory audit coverage via partner: the Reg 3(p) defined term requires a CERT-In empanelled auditor for every statutory audit (annual, pre-commissioning, web-app clearance). Strategy: partner with an empanelled firm - Shieldworkz delivers the OT-competent assessment, evidence packs and remediation; the partner signs the statutory report. This converts the empanelment gap into a channel: empanelled firms are IT-audit-centric and lack OT depth, making Shieldworkz the natural OT execution arm. Structure as revenue share on the audit fee plus full ownership of the pre/post-audit work (R1-R4), which carries the margin. Pursue own empanelment in parallel as a medium-term de-risk
- Indian procurement reality: PSU purchases route through GeM listing and tenders with L1 pricing pressure - counter with the SLDC/state repeatable pack (fixed-price, fixed-scope) and OEM/SI partnerships for tender access; private Tiers 1 and 3 buy direct
- Delivery capacity: ~45 assessments plus 30 documentation suites needs 4-6 delivery consultants leveraged by the AI generation pipeline - the pipeline is the margin engine; without it this plan needs double the headcount
- Local presence: an India entity or partner for PSU contracting, data-residency assurance and CSIRT-Power ecosystem participation
- Competition: Big-4 and Indian IT majors will chase the consulting layer; global OT platforms will chase Tier 1 - the defensible ground is the integrated product (assessment + generation + registers + cockpit) at India-viable price points, which none of them will build for a single-country regulation

- Timing risk: enforcement slippage past April 2027 would delay conversion - mitigated because audit cycles, RDSS conditionality and Protected System criminal exposure operate independently of penalty enforcement

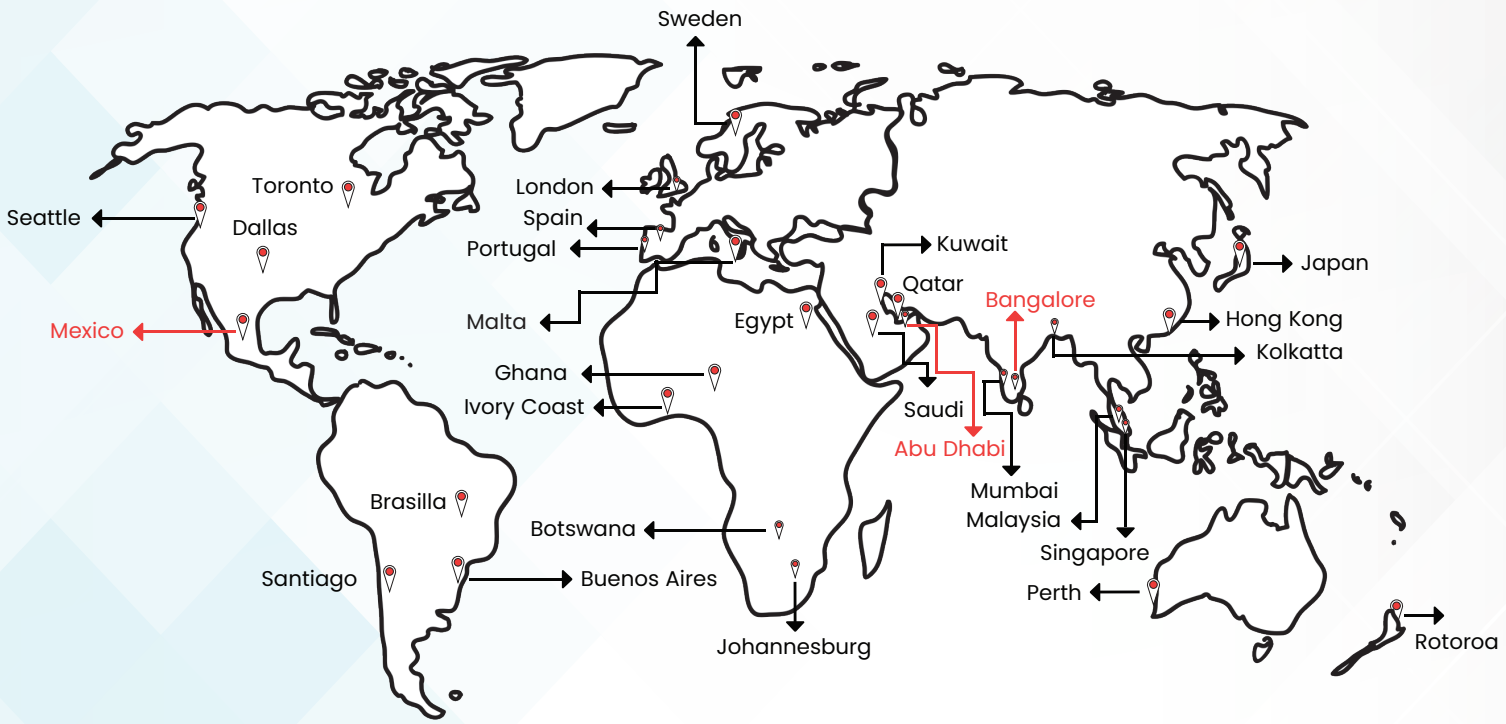
19. Immediate Actions

- Sign a CERT-In empanelled audit partner now (target: an empanelled firm with power-sector clients but thin OT bench) - this unlocks statutory audit participation immediately; pursue own empanelment in parallel as a medium-term de-risk
- Build the CEA 2026 to IEC 62443 control-mapping matrix - the foundation artifact for the framework pack (weeks of work)
- Repoint the AI generation pipeline at the Reg 8 policy suite - the differentiator no competitor ships
- Stand up the SLDC/state repeatable pack at a fixed price and open the first three SLDC conversations
- Open Tier 1 audit-preparation conversations ahead of Q4 2026 budget cycles; anchor on Grid-India, Powergrid and one integrated private (Tata Power or Adani)
- Establish the India contracting entity/partner and GeM listing
- Track CEA separate orders on the six deferred provisions - each order is a discrete sales trigger, especially 6(2) perimeter hardware and the trusted-source mechanism

---

Prepared by Shieldworkz OT Systems. Sources: Gazette of India Extraordinary No. 484 (31 July 2026); CEA Cyber Security Guidelines 2021; public market data. This document contains forward-looking commercial estimates for internal planning purposes.

About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Copyright @ 2026, Shieldworkz - All rights Reserved.

Contact Us

GERMANY

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

CANADA

396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada

+1 (437) 223-7770

americas@shieldworkz.com

UAE

Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com

INDIA

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com

Copyright @ 2026, Shieldworkz - All rights Reserved.