CHECKLIST

SHIELDWORKZ

CEA 2026 Compliance Checklist

Client Working Copy - Part A: Required by 1 April 2027 | Part B: Ongoing Obligations

Shieldworkz OT Systems | August 2026 | SWZ-REF-REG-202608-003

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

Scope: all covered entities (generators ≥50 MW, transmission and distribution licensees, NLDC/RLDCs/SLDCs; exchanges are exempt from OT items marked Reg 6). Deferred provisions 5(9), 5(24), 5(33), 5(39), 6(2), 6(7) are excluded from Part A and listed in Part C as watch items. Enter owner, status and target date against each item; each unchecked box at the end of an assessment is a remediation scope line.

Part A - Required by 1 April 2027

A1. Governance and Organisation

	Item	Reg	Owner / Status / Date
	Designate CISO and alternate CISO: regular senior-management employees; engineering degree; 15 yrs power/IT experience; Indian citizen and resident; min 3-year tenure; role ring-fenced to cyber only	5(1)-(6), 7(1)	_____
	CISO reporting line to head of entity (holding-company head for SLDC-type entities)	5(4)	_____
	Publish CISO + alternate contact details; communicate to CSIRT-Power and all stakeholders	5(7)	_____
	Schedule 5 man-days/yr CISO cyber security training (first FY cycle)	5(8)	_____
	Designate board/senior-management member accountable for regulatory compliance (recommended)	15	_____

A2. Policy and Plan Suite (board approval cycles - longest documentation lead)

	Item	Reg	Owner / Status / Date
	Cyber Security Policy drafted covering all 33 Reg 8 elements; head/board approved	5(10), 8	_____
	Business Continuity Plan aligned; criticality-classification criteria derived from it	8, 8(5)	_____
	Cyber Crisis Management Plan: drafted in consultation with CSIRT-Power; submitted for CERT-In vetting (START FIRST - external queue); head/board approved	5(11), 9	_____
	Incident Response & Recovery Plan (incident taxonomy, risk-based response plans, crisis classification criterion)	5(35), 8(9)	_____
	Data Retention Policy (all Reg 8(33) categories and floors)	8(33)	_____
	Backup Policy (≤1 month currency; integrity/restoration testing defined)	8(18)	_____
	Digital data protection & privacy policy	8(17)	_____

	Item	Reg	Owner / Status / Date
	Internet access policy	8(21)	_____
	Remote access procedure (least privilege, minimum duration, MFA, geo-fencing, approval authority matrix)	5(17), 8(15)	_____
	Remote operation procedure (India-only, board approval path, dedicated channel)	6(4), 8(16)	_____
	Change management process (two-category update classification per Second Schedule; version control + rollback; OEM-signed OT patches; simulated testing; offline deployment)	8(24)-(25)	_____
	Supply-chain risk management process	8(14)	_____
	Obsolete-asset phase-out plan + secure disposal procedures (assets and sensitive data)	8(22), 8(31)-(32)	_____
	Personnel risk assessment process (vendor staff; role-change and post-exit triggers)	8(12)	_____

A3. Registers, Classification and Risk Baseline

	Item	Reg	Owner / Status / Date
	Deploy passive discovery (Shieldworkz NDR sensors) to build the asset baseline without touching live OT	supports 5(25)	_____
	Cyber asset register: every cyber asset with ownership, hardware, firmware, software, patch status	5(25)(a)	_____
	Critical systems register: configuration, hardware/software, network architecture with data flows, communication protocols	5(25)(b)	_____
	Critical / non-critical classification executed per BCP-impact criteria; recorded in register	5(16), 8(5)	_____
	Cyber Risk Assessment & Mitigation Plan: per-asset vulnerabilities, threats, risks, controls - implemented, not just written	5(26), 8(6)	_____
	Personnel risk assessments completed for all vendor staff with critical-system access; SLA undertakings collected	5(20), 8(12)	_____
	Initiate NCIIPC CII identification; diarise 60-day Protected System window on identification	5(29)	_____
	Verify CII/Protected Systems not discoverable on public platforms (or board-approved exception documented)	5(30)	_____

A4. Architecture and Engineering (longest lead - start first)

Item	Reg	Owner / Status / Date
Map every IT/OT interconnection and internet touchpoint (NDR traffic analysis provides evidence)	precursor to 6(1)	
OT physically isolated from internet and IT; OR each interconnection risk-assessed, hardened logical separation implemented, board approved, continuously monitored, logs retained	6(1)	
IT networks containing CII separated from internet and other IT networks; hardened sourcing where internet unavoidable	5(12)	
ESP security devices deployed and configured (DPI, encrypted-traffic inspection, IDS/IPS, geo-fencing, content/user/app filtering, anomaly detection) - NOT deferred; only 6(2) OT-interconnection devices are	5(13)	
Security devices for all critical web applications (application-layer filtering, bidirectional protection)	5(15)	
Physical-security systems/networks separated from critical-system networks (logical separation with head approval where physical infeasible)	5(34)	
Power-system control/real-time data confined to dedicated internet-isolated channels within national boundaries; cross-border flows via dedicated systems + unidirectional gateways; end-consumer data on secured encrypted connections	6(3)	
OT communication system isolated from IT communication system	6(6)	
OT environment segmented into trust levels (criticality, security requirements, risk assessment)	6(8)	
Sensitive data inventory; encryption at rest; confirm India-only residency incl. cloud and historical data; repatriate offshore data	5(19)	
Online + offline backups of all critical systems operating in separate secure environment; restoration tested	5(21), 8(18)	
Logging enabled on all ESP devices; log storage mechanism per retention policy	5(37), 8(26)	
Reference time source selected after cyber risk assessment (OT: terrestrial or India-specific satellite, internet-independent); clocks synchronised	5(32), 8(27)	

A5. Operational Processes Live Before Day One

Item	Reg	Owner / Status / Date
Continuous monitoring of IT and OT systems operational (Shieldworkz NDR): passive, behaviour-baselined, Purdue-contextualised - needs operating history before first audit	5(36)	
Incident detection-to-report workflow tested: 6-hour standard / 24-hour sabotage timelines to CSIRT-Power and CERT-In; report templates ready	7(3)(a)	
Incident register established in CSIRT-Power prescribed format; NDR detections feed it	5(42)	
Vendor SLAs renegotiated: cyber requirements + NDA embedded, survival clauses; undertakings from vendors with critical-system access	5(20)	
Structured vulnerability disclosure and management programmes stood up with vendors and CSIRT-Power	5(41)	

	Item	Reg	Owner / Status / Date
	FAT/SAT with cyber security test scope embedded in procurement templates	5(31)	_____
	First cyber security awareness programme + mock drill/tabletop delivered (starts the 6-month clock)	5(18)	_____
	IT products procurement compliance with Central Government orders verified	5(23)	_____
	Public IP inventory (allocated/used/unused) compiled for CSIRT-Power	7(3)(l)	_____
	IT Act 2000 compliance review (directions and subordinate rules, incl. CERT-In 2022 direction)	5(40)	_____

Part B - Ongoing Obligations (from 1 April 2027)

B1. Recurring Calendar

	Obligation	Reg	Frequency + Status
	Cyber security incident reporting: 6 hours (standard) / 24 hours (concluded sabotage in critical systems) to CSIRT-Power + CERT-In, with ATRs and root-cause analyses to follow	7(3)(a),(g)	Continuous _____
	Continuous IT/OT monitoring; surveillance for threats and vulnerabilities; incident response and remediation	5(36)	Continuous (24x7) _____
	Quarterly review of policy-mandated compliances	7(3)(b)	Quarterly _____
	Random testing of critical-system day-to-day operations for policy conformance; corrective measures	7(3)(m), 8(10)	Ongoing programme _____
	Cyber Risk Assessment & Mitigation Plan update	5(26)	Every 6 months _____
	Incident Response & Recovery Plan review and update	5(35)	Every 6 months _____
	Awareness programme + cyber exercise (mock drill / tabletop)	5(18)	Every 6 months _____
	Comprehensive cyber security audit by CERT-In empanelled auditor (via audit partner): all critical systems; 9-15 month spacing; rotate after 3 consecutive; findings closed 1 month (critical/high) / 3 months (medium/low); closure report within 6 months	5(22), 13, 14	Annual - first in FY27-28 _____
	Self-audit against all applicable regulations; non-compliances closed before next FY's self-audit	15	Annual _____
	Cyber Security Policy review and re-approval by head/board	5(10)	Annual _____
	CCMP review, re-approval; efficacy test via drills on non-repeating scenario selection	5(11), 10(2)	Annual _____
	Asset registers review (also triggered by any commissioning/replacement)	5(25)	Annual _____
	Criticality-classification procedure, risk procedure, vulnerability-management mechanism reviews	8(5)-(7)	Annual _____
	Perimeter security device rules and policies review	5(38)	Annual _____
	Backup policy + data retention policy review; backup integrity and restoration testing	8(18), 8(33)	Annual _____
	Remote operation procedure review (or on business change, whichever first)	8(16)	Annual _____
	Annual training: CISO 5 man-days; all personnel with critical-system access per training programme	5(8), 8(20)	Annual _____
	Certification maintenance once 5(24) commences: ISO 27001/TCC surveillance audits; 4-audit rotation	5(24)	Per cert cycle _____

B2. Event-Triggered Obligations

	Trigger and Required Action	Reg	Window + Status
	New/replaced critical system: pre-commissioning cyber security audit incl. VAPT BEFORE go-live	5(27)	Every commissioning _____
	New/replaced critical system: details to CSIRT-Power within 30 days; asset registers updated	5(28), 5(25)	30 days _____
	New public-facing web service/portal/API: audit clearance before deployment	5(14)	Every deployment _____
	Software updates: classify per Second Schedule criteria - prior-audit category cleared before deployment; others assessed at next audit; OT patches OEM-signed, tested in simulation, deployed offline	5(14), 8(24)-(25)	Every update _____
	Remote access grant to critical system: comprehensive risk assessment, approval, continuous monitoring; records + logs retained 1 year	5(17)	Every grant _____
	NCIIPC identifies an asset as CII: approach Appropriate Government for Protected System notification within 60 days; implement NCIIPC-validated controls	5(29), 7(3)(d)	60 days _____
	Actual cyber crisis: execute CCMP with CSIRT-Power coordination; detailed report (handling, lessons, lapses, measures); share with CSIRT-Power; update CCMP	10(3)	Per crisis _____
	Cyber security breach by vendor: enquiry + action against vendor incl. cloud providers	5(20)	Per breach _____
	Directives/advisories from Central Govt, CEA, CERT-In, CSIRT-Power: act upon	7(3)(e)	As issued _____
	CISO/alternate change: succession without simultaneous vacancy; re-publish details	5(2), 5(7)	Per change _____
	Vendor staff role change or exit (termination/resignation/superannuation): personnel risk assessment	8(12)	Per event _____
	CISO-MoP demands audit closure report / verifies self-audit: respond; third-party verification at entity cost if appointed	14(2), 15	On demand _____

B3. Standing Retention Floors (evidence the auditor checks)

	Record	Reg	Retention + Status
	Last two working data backups of critical systems always available	8(33)(a)	Standing _____
	Remote-access risk assessments, physical approval records, logs	8(33)(b)	1 year _____
	IT-OT interconnection approvals and logs	8(33)(c)	Per retention policy _____
	FAT/SAT reports incl. cyber tests	8(33)(c)	Life of asset _____
	Remote-operation risk assessments and approvals	8(33)(d)	1 year _____
	Cyber security audit reports	8(33)(e)	3 years _____
	Certification audit reports	8(33)(f)	4 years _____

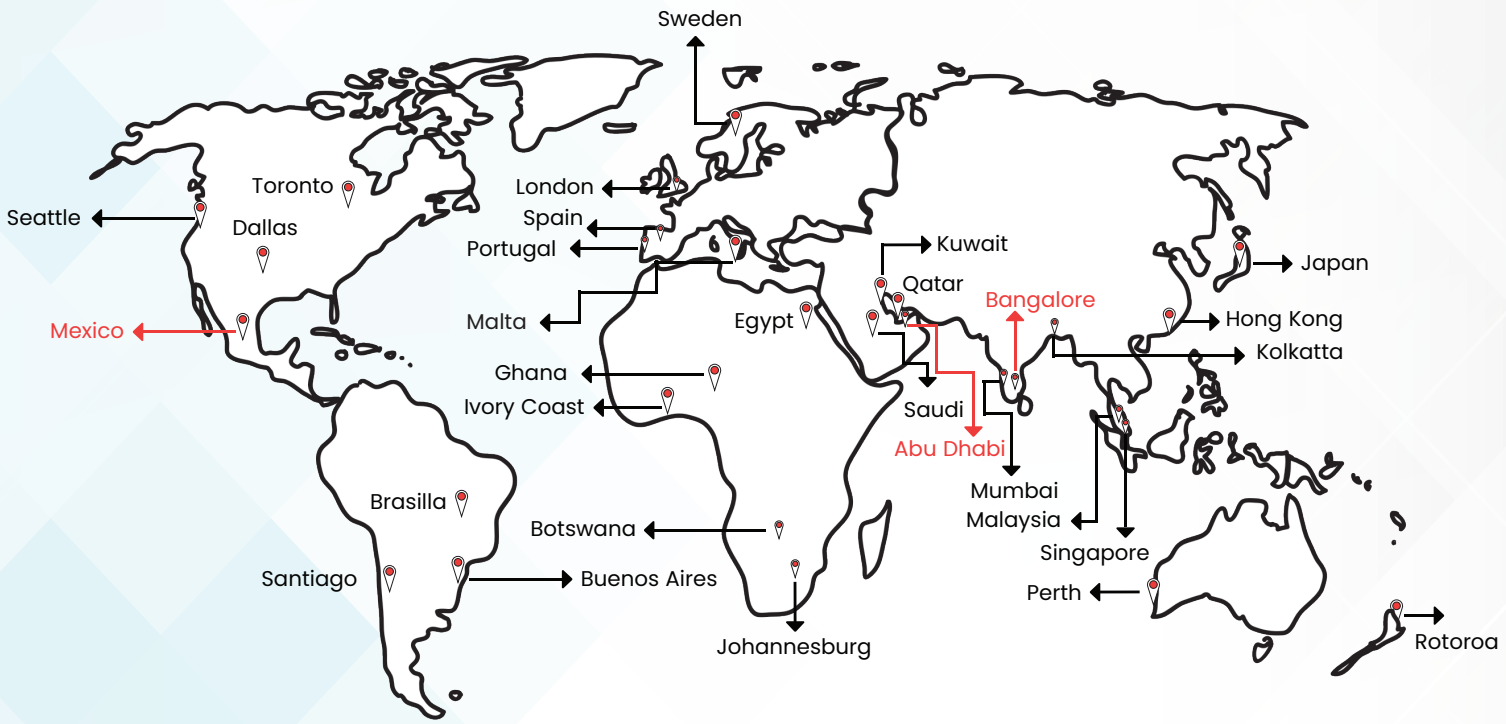
	Record	Reg	Retention + Status
	Self-audit reports	8(33)(g)	3 years
	All ICT + IT-OT interconnection logs and forensic records	8(33)(h)	180 days
	Incident-associated logs (180 days pre and post incident)	8(33)(i)	365 days from incident
	First Schedule document custody with CISO (CSP, CCMP, retention policy, certificates, registers, risk plan, IR&R;, incident register, SBOM, BCP, remote procedures)	7(3)(i)	Standing

Part C - Deferred Provisions Watch List (separate CEA orders)

	Deferred Requirement	Reg	Trigger + Status
	24x7 Information Security Division in India: certified staff, 3-year postings, 5 man-days/yr training - pre-plan headcount/managed-SOC model now	5(9)	On CEA order
	ISO/IEC 27001 or Technical Criteria Certificate for all critical systems - begin gap work early; certification cycles run 6-12 months	5(24)	On CEA order
	Designated power-sector cyber courses for all personnel incl. vendor O&M; staff	5(33)	On CEA order
	Trusted-source procurement - IT equipment and services	5(39)	On CEA order
	OT-protocol-aware perimeter devices at every OT interconnection point; offline-only signature updates - budget the hardware cycle now	6(2)	On CEA order
	Trusted-source procurement - OT equipment and services	6(7)	On CEA order

Critical-path guidance: begin with A4 architecture items and the CCMP CERT-In vetting submission (the two longest external/engineering leads), and deploy passive monitoring (A5, 5(36)) early - it is the only Part A item that cannot be satisfied by documentation and simultaneously auto-populates the A3 registers. Shieldworkz OT Systems | SWZ-REF-REG-202608-003

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.