This checklist summarises CERT-In's **15 Elemental Cyber Defense Controls for Micro, Small and Medium Enterprises (MSMEs)**, Version 1.0 dated 01.09.2025, and the 45 Security Baseline Recommendations mapped to them. Use it to self-assess your readiness and to prepare for a baseline audit. It applies to enterprises meeting the MSME classification under Notification No. S.O. 1702(E) dated 1 June 2020 (MSMED Act, 2006). CERT-In states these controls are a **minimum baseline** — not a complete security programme. Tick each item you can evidence today; anything unticked is your roadmap.

Statutory obligations that sit alongside the 15 controls

- **6-hour incident reporting:** report listed cyber incidents (Annexure I of the 28.04.2022 Directions) to CERT-In within 6 hours — incident@cert-in.org.in / 1800-11-4949.
- **180-day logs:** enable ICT system logs and retain them for a rolling 180 days within Indian jurisdiction.
- **Time sync:** synchronise all system clocks to NIC or NPL NTP servers.
- **Annual baseline audit:** conduct a baseline audit of these controls through a CERT-In Empaneled Auditing Organization at least once a year.

The 15 controls & 45 baseline recommendations

1. Effective Asset Management (EAM)

- ☐ **EAM.1** Maintain a centralized, continuously updated inventory of all hardware, software and information assets; identify, label and classify sensitive assets for appropriate handling and access control.
- ☐ **EAM.2** Track the full asset lifecycle — acquisition, deployment, use and secure disposal — updating records on any change in location, status or condition.

2. Network and Email Security (NES)

- ☐ **NES.1** Deploy firewalls at the network perimeter and enable host-based firewalls; ensure they are properly configured.
- ☐ **NES.2** Secure Wi-Fi with WPA2/WPA3, strong passwords and hidden SSIDs; avoid factory-default credentials; segregate guest networks; prevent devices from auto-connecting to open/public Wi-Fi.
- ☐ **NES.3** Implement VPNs with encryption and MFA to secure remote access.
- ☐ **NES.4** Protect email and messaging from phishing and spoofing using SPF, DKIM and DMARC.

3. Endpoint & Mobile Security (EMS)

- ☐ **EMS.1** Install licensed antivirus / endpoint protection on all devices; keep built-in OS security (e.g. Windows Defender, Firewall) enabled.
- ☐ **EMS.2** Avoid pirated or unauthorized software; restrict software installation to authorized personnel only.
- ☐ **EMS.3** Onboard with CERT-In's Cyber Swachhta Kendra (CSK), the Botnet Cleaning and Malware Analysis Centre, to receive malware/botnet alerts and advisories.
- ☐ **EMS.4** Restrict or control USB and removable-media usage; disable autorun to prevent malware spread.

4. Secure Configurations (SC)

- [ ] **SC.1** Implement and maintain approved baseline security configurations for servers, endpoints, network devices, browsers and commercial off-the-shelf (COTS) software.
- [ ] **SC.2** Disable unnecessary features, ports, services, protocols and default applications to reduce the attack surface.
- [ ] **SC.3** Remove unused software and system functions; change all default passwords and settings before deployment.

5. Patch Management (PM)

- [ ] **PM.1** Regularly apply security patches and updates to operating systems, applications and firmware.
- [ ] **PM.2** Monitor vendor notifications, CERT-In advisories and other sources to stay informed of patches and vulnerabilities affecting your IT environment.

6. Incident Management (IM)

- [ ] **IM.1** Develop and document a formal Incident Response Plan (IRP) covering reporting, containment, investigation, recovery and communication.
- [ ] **IM.2** Conduct regular testing of the IRP to ensure effectiveness and readiness during actual incidents.
- [ ] **IM.3** Adhere to CERT-In's 28.04.2022 Directions under §70B(6) — including reporting cybersecurity incidents to CERT-In within 6 hours of detection or notification.

7. Logging and Monitoring (LM)

- [ ] **LM.1** Enable comprehensive logging on all key ICT systems; retain system and application logs for a minimum of 180 days with secure storage within Indian jurisdiction.
- [ ] **LM.2** Continuously monitor network activity and privileged-user actions to detect suspicious behaviour and unauthorized access attempts.
- [ ] **LM.3** Deploy monitoring security solutions to enhance log analysis, threat detection and response.

8. Awareness and Training (AT)

- [ ] **AT.1** Conduct basic cybersecurity awareness training at least twice a year for all employees and contractors — phishing, password hygiene, social engineering, BYOD, safe internet use, acceptable use and handling of sensitive information.
- [ ] **AT.2** Participate in CERT-In awareness workshops, capacity-building programs and national-level cybersecurity exercises and drills.

9. Third Party Risk Management (TPRM)

- [ ] **TPRM.1** Conduct thorough due diligence on each vendor or third party based on potential business impact or likelihood of compromise.
- [ ] **TPRM.2** Hold all third-party providers to at least the same security standards applied internally (this baseline), ensuring consistency across the supply chain.

10. Data Protection, Backup and Recovery (DPBP)

- [ ] **DPBP.1** Keep a regular backup schedule with encrypted copies stored in secure, separate sites — combining offsite and offline media (e.g. USB or tape).
- [ ] **DPBP.2** Periodically test backup restoration to ensure data recoverability and system resilience.
- [ ] **DPBP.3** Develop and maintain a minimum Business Continuity Plan (BCP) for identified critical applications.
- [ ] **DPBP.4** Ensure secure disposal of physical and digital media using proper sanitization or destruction methods.

11. Governance and Compliance (GC)

- [ ] **GC.1** Assign a security in-charge / single point of contact to oversee information security and serve as the primary contact for CERT-In and regulators.
- [ ] **GC.2** Establish and formally approve an Information Security Policy covering data protection, access control, incident response, passwords, third-party management and audits.
- [ ] **GC.3** Periodically review and update security policies to reflect major business, technological or regulatory changes.
- [ ] **GC.4** Adhere to guidelines and directions issued by CERT-In and regulators.

12. Robust Password Policy (RPP)

- [ ] **RPP.1** Enforce strong, unique passwords (minimum 8–12 characters, mixed character types) with expiry intervals and no reuse; educate users against sharing credentials.
- [ ] **RPP.2** Temporarily lock accounts after 3–5 failed login attempts to prevent brute-force attacks.
- [ ] **RPP.3** Enable Multi-Factor Authentication (MFA) for all critical systems, administrative accounts and remote-access tools.
- [ ] **RPP.4** Store passwords securely using strong encryption and hashing algorithms.

13. Access Control and Identity Management (ACIM)

- [ ] **ACIM.1** Assign unique user IDs to all individuals — no shared accounts — to ensure full traceability of system activity.
- [ ] **ACIM.2** Implement role-based access controls aligned to job responsibilities, following the principle of least privilege.
- [ ] **ACIM.3** Review and update access privileges at least quarterly, and immediately on role change, transfer or exit, using a formal offboarding checklist.
- [ ] **ACIM.4** Grant administrative privileges only when essential; enforce segregation of duties across administrative, financial and data functions.

14. Physical Security (PS)

- [ ] **PS.1** Implement physical access controls for critical infrastructure — security guards, electronic badges and biometric access for server rooms and network equipment; monitor entry/exit with CCTV.
- [ ] **PS.2** Maintain an asset-return checklist (ID cards, laptops, USB drives, equipment) for every employee exit.

15. Vulnerability Audits and Assessments (VAA)

VAA.1 Ensure independent third-party vulnerability assessments of business-critical assets and applications at least once a year, with timely remediation. ☐

VAA.2 Perform periodic risk assessments to identify organization-specific threats and guide mitigation strategies. ☐

How to use this checklist

- **Score each recommendation** 0 (nothing) to 3 (mature and documented) — not just the 15 headline controls.
- **For every 0 or 1,** write a one-line remediation and a target date.
- **Collect evidence** an auditor will ask for: asset inventory, access-review records, change/patch logs, the IRP and 6-hour reporting template, vendor register, backup-restore results, and the approved security policy.
- **Run an internal pre-audit** before paying for an external pass through a CERT-In Empaneled Auditing Organization.

Read the full guide at the GRC RADAR hub (/grc-radar/). Questions on how a control applies to your MSME? Ask via /contact/.