xloTz Cyber Assurance Platform

CERT-In MSME Compliance Checklist

The practitioner's guide from the team that helped shape India's CERT-In MSME Cybersecurity Baseline

xloTz

Written by practitioners, not observers. xloTz contributed directly to developing India's CERT-In MSME Cybersecurity Baseline. Use this checklist to assess your current compliance posture against all 15 Elemental Cyber Defense Controls.

The Non-Negotiables

These are enforceable legal obligations under India's IT Act and CERT-In directives — not optional guidelines.

	Implement all 15 Elemental Cyber Defense Controls in full	[ ]
	Retain system logs for at least 180 days, stored within India	[ ]
	Report major cyber incidents to CERT-In within 6 hours of detection	[ ]
	Conduct cybersecurity awareness training at least twice a year	[ ]
	Complete an independent vulnerability assessment annually	[ ]
	Undergo audits by CERT-In empaneled auditors only	[ ]

Rs.1 Cr Maximum fine per violation

6 Hours Incident reporting window

180 Days Minimum log retention

CERT-In MSME Compliance Checklist: The 15 Controls

Rate your current status for each control. Use the status column to mark: Done / In Progress / Not Started.

#	Control	Category	Status	Owner
01	**Effective Asset Management** Know every device, software, and data asset. Track from day one to secure disposal. Nothing unknown should exist on your network.	OPERATIONAL	_____	_____
02	**Network & Email Security** Proper firewalls. Secure Wi-Fi (WPA2/WPA3). VPN and MFA for remote access. Email protection via SPF, DKIM, DMARC.	TECHNICAL	_____	_____

#	Control	Category	Status	Owner
03	**Endpoint & Mobile Security** Licensed antivirus on every device. No pirated software. USB restrictions. Built-in OS security features switched on.	TECHNICAL	_____	_____
04	**Secure Configurations** Configure every server, endpoint, and application securely before go-live. Disable what you don't use. Defaults are not safe.	TECHNICAL	_____	_____
05	**Patch Management** Update regularly — OS, applications, firmware. Unpatched systems are open doors. Attackers scan for known vulnerabilities within hours.	CRITICAL	_____	_____
06	**Incident Management** Have a plan before you need one. Detection, response, investigation, recovery — all mapped out. Report to CERT-In within 6 hours.	CRITICAL	_____	_____
07	**Logging & Monitoring** Record what's happening across your systems. Monitor for unusual behaviour. Retain logs 180 days, stored within India.	CRITICAL	_____	_____
08	**Awareness & Training** Train your team at least twice a year — phishing, passwords, data protection, social engineering. People are your first line of defence.	GOVERNANCE	_____	_____
09	**Third-Party Risk Management** Your vendors inherit your risk. Evaluate their security. Hold them to the same standards — and get it in writing.	GOVERNANCE	_____	_____
10	**Data Protection, Backup & Recovery** Encrypted backups, stored offline or offsite. Test recovery regularly. If you can't restore it, the backup doesn't count.	CRITICAL	_____	_____
11	**Governance & Compliance** Appoint someone responsible for cybersecurity. Have an approved security policy. Follow regulatory guidelines. Ownership matters.	GOVERNANCE	_____	_____
12	**Robust Password Policy** Strong passwords. Account lockouts after failed attempts. MFA on everything critical. Reused passwords are a breach waiting to happen.	TECHNICAL	_____	_____

xiotz.com +91 - 9980615581 sales@xiotz.com

#	Control	Category	Status	Owner
13	**Access Control & Identity Management** Unique user IDs. Access based on role. Permissions reviewed regularly. Revoke access immediately when someone leaves.	TECHNICAL	_____	_____
14	**Physical Security** Server rooms need controlled access. CCTV. Badges. Biometrics. Digital security fails when physical security doesn't exist.	OPERATIONAL	_____	_____
15	**Vulnerability Audits & Assessments** Independent assessment annually by CERT-In empaneled auditor. Fix what's found. The audit is not the finish line — remediation is.	CRITICAL	_____	_____

How to Use This Checklist

8-10 controls met	Baseline in place. Focus on closing the remaining gaps — especially logging, incident response, and third-party risk.
5-7 controls met	Significant exposure. Prioritise Controls 5, 6, 7, and 10 immediately — these are the most commonly exploited gaps.
Below 5 controls	High risk. You need a structured implementation plan. xIoTz can deploy a unified compliance platform in under 2 hours.

xiotz.com +91 - 9980615581 sales@xiotz.com