THE POWER OF BEING UNDERSTOOD

RSM

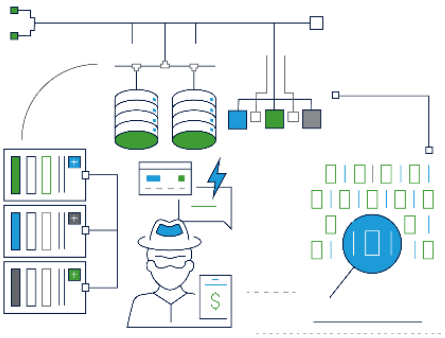
Newsflash –Key Aspects of the 15 Elemental Cyber Defense Controls for Micro, Small and Medium Enterprises by CERT-In *(Notification dated 1st September 2025)*

Newsflash
Key Aspects of the 15 Elemental Cyber Defense Controls for Micro, Small and Medium Enterprises by CERT-In
(Notification dated 1st September 2025)

For Circulation
19 September 2025

1.0 Background

Cyber security is important for Micro, Small and Medium Enterprises (MSMEs) for the purpose of safeguarding cyber infrastructure, confidentiality, integrity and availability of data, reduce operational downtime, reduce financial risk, support digital projects, maintain customer confidence, build brand image and ensure legal compliance. In order to help them attain such security, CERT-In, has provided a set of 15 elemental controls against which such companies may benchmark their cyber security and eventually build upon a comprehensive organization wide cyber security framework.



2.0 CERT-In

CERT-In is an acronym for “Indian Computer Emergency Response Team” and is a functional organization of Electronics and Information Technology, Government of India, with the objective of securing the Indian cyber space. CERT-In provides Incident prevention and Response services as well as Security Quality Management services.

3.0 Cyber Defense Controls & Security Baseline recommendations for implementation

CERT-In has provided 15 baseline controls mapped to 45 recommendations which can be implemented as baseline cyber security defense mechanism. MSMEs may conduct baseline audits by CERT-In empaneled organizations at least annually and continually improve the cybersecurity posture of the organization.

The 15 controls and their mapped recommendations are as follows:

i. Effective Asset Management (EAM)
- a. Maintain a centralized, updated inventory of all assets.
- b. Track full asset lifecycle from acquisition to disposal.

ii. Network and Email security (NES)
- a. Deploy firewalls
- b. Ensure wireless network is properly secured
- c. Implement VPN with encryption and MFA
- d. Protect email and messaging systems

iii. **Endpoint and Mobile security (EMS)**
   a. Install antivirus or endpoint protection on all devices
   b. Avoid pirated or unauthorized software
   c. On-board with CERT-In's CSK
   d. Restrict or control USB and removable media usage

iv. **Secure Configurations (SC)**
   a. Implement and maintain baseline security configuration
   b. Disable unnecessary features, ports, services, applications, etc.
   c. Remove unused software and system functions

v. **Patch Management (PM)**
   a. Regularly apply and update patches
   b. Monitor vendor notifications and security updates/advisory

vi. **Incident Management (IM)**
   a. Develop and document a formal incident response plan (IRP)
   b. Conduct regular test of IRP
   c. Adhere to directions under sub-section (6) of section 70B of the Information Technology Act, 2000

vii. **Logging and Monitoring (LM)**
   a. Enable logging and maintain logs for minimum 180 days
   b. Continuous monitoring of network and privileged user activity
   c. Deploy monitoring security solutions

viii. **Awareness and Training (AT)**
   a. Conduct cyber security awareness trainings at least twice a year
   b. Actively participate in cyber security workshops

ix. **Third Party Risk Management (TPRM)**
   a. Conduct thorough due diligence for each vendor
   b. Hold all third-party providers to the same security standards applied internally

x. **Data Protection, Backup and Recovery (DPBP)**
   a. Establish a regular backup schedule
   b. Test backup restoration procedures periodically
   c. Develop and maintain a minimum Business Continuity Plan (BCP)
   d. Ensure secure disposal of media

xi. **Governance and Compliance**
   a. Assign SPOC for all information security activities
   b. Establish and approve Security Information Policy
   c. Periodically update Security Policies
   d. Adhere to guidelines issued by CERT-In

xii. **Robust Password Policy (RPP)**
   a. Enforce strong password usage
   b. Temporarily lock accounts after 3 to 5 failed attempts
   c. Enable MFA
   d. Use secure encryption and hashing algorithms for password storage

xiii. Access Control and Identity Management (ACIM)

a. Assign unique user IDs
b. Implement role-based access controls
c. Review and update user access privileges regularly
d. Grant administrative privileges only where required

xiv. Physical Security (PS)

a. Implement robust access controls for critical infrastructure and systems
b. Maintain a comprehensive asset-return checklist

xv. Vulnerability Audits and Assessments (VAA)

a. Ensure independent third-party vulnerability assessments are conducted atleast annually
b. Perform periodic risk assessments to identify risks and mitigate them

4.0 Conclusion

In an era where digital transformation is vital for business growth, Micro, Small, and Medium Enterprises (MSMEs) must prioritize cybersecurity to safeguard their operations, data, and customer trust. The 15 Elemental Cyber Defense Controls outlined by CERT-In serve as a foundational framework and a starting point to help MSMEs establish a robust cybersecurity posture.

CERT-In encourages MSMEs to integrate these controls into their cybersecurity policies, conduct annual baseline audits through empanelled auditing organizations, and stay updated with emerging threats and best practices. While these elemental controls provide a strong starting point, MSMEs are advised to evolve their cybersecurity strategies in alignment with their specific risk profiles, industry standards, and technological advancements.

By embracing this framework, MSMEs can confidently navigate the digital landscape, protect their assets, and contribute to a secure and resilient cyber ecosystem in India.

For further information please contact:

RSM Astute Consulting Pvt. Ltd.

8th Floor, Bakhtawar, 229, Nariman Point, Mumbai - 400021.

T: (91-22) 6108 5555/ 6121 4444
F: (91-22) 6108 5556/ 2287 5771

E: emails@rsmindia.in **W:** www.rsmindia.in

Offices: Mumbai, New Delhi - NCR, Chennai, Kolkata, Bengaluru, Navi Mumbai, Surat, Hyderabad, Ahmedabad, Pune, Gandhidham, Jaipur and Vijayanagar.

 facebook.com/RSMinIndia

 X.com/RSM_India

 linkedin.com/company/rsm-india

 Youtube.com/c/RSMIndia

19 September 2025