Deloitte.

CERT-In guidelines on information security practices for government entities

August 2023

Table of contents

Introduction

With Information and Communication Technologies (ICT) now entrenched in almost every facet of service delivery and operations, continuously evolving cyber threats have become a concern for the Indian government. To protect ICT against cyber threats, the Indian Computer Emergency Response Team (CERT-In), recently issued guidelines on Information Security practices for government entities[1] in-line with the Government of India's objective to ensure that digital nagriks[2] experience a safe and trusted internet. These guidelines serve the following purposes:

Establish a prioritised baseline for cybersecurity measures and controls, within government organisations and their associated entities.

Assist security teams to implement baseline, and essential controls and procedures to protect their infrastructure from prominent threats.

Act as a foundational document for administration and audit teams (internal, external/ third-party auditors).

In addition to the generic directives issued to government entities, these guidelines include specific dos and don'ts for central government CISOs and employees from the National Informatic Centre (NIC) (included in Annexure 1 of the guideline).

The main part of the guideline covers 15 domains in information security. It has one annexure (guidelines for central government CISOs and employees - issued by National Informatics Centre). The annexure consists of two parts:

Part - 1 Guideline for CISOs of central government ministries/departments

Part - 2 Cybersecurity guidelines for government employees

The guideline also has two appendices:

Appendix 1 - Security compliance checklist

Appendix 2 - Network architecture

[1] Ministries, departments, secretariats, and offices specified in the First Schedule to the Government of India (Allocation of Business) Rules, 1961, their attached and subordinate offices, and government institutions, public -sector enterprises, and other government agencies under their administrative purview.

[2] Indians (Digital Nagrik) presently connected and using internet and cyberspace.

Structure of the CERT-In guidelines

Guidelines on information security practices for government entities

1. Introduction and purpose
2. Applicability and scope
3. Policy measures
4. Network and infrastructure security
5. Identity and access management
6. Application security
7. Data security
8. Third-party access and outsourcing
9. Secure cloud services
10. Hardening procedures
11. User awareness and training
12. Social media security
13. Vulnerability and patch management
14. Security monitoring and incident management
15. Security auditing guidelines

Annexure 1: Guidelines for central government CISOs and employees (issued by National Informatics Centre)

Part 1:[3] Guideline for CISOs of central government ministries/ departments

- Scope
- Secure local area network
- Secure wireless LAN network
- Desktop/laptop and printer security
- Server security
- Logging
- Compliance

Part 2:[4] Cyber security guidelines for government employees

- Scope and target audience
- Desktop/laptop and printer security at office
- Password management
- Internet browsing security
- Mobile security
- Email security
- Removable media security
- Social media security
- Security advisory and incident response
- Cyber security resources
- Compliance

Appendix - 1: Security compliance checklist

Appendix - 2: Network architecture

[3] Shall be adhered to by the respective IT/network teams of each ministry/department. The CISO of the ministry/department shall ensure compliance of these guidelines.

[4] To be adhered by government employees, including outsourced/contractual/temporary employees who work for government ministry/department.


3628 1820 1458
2636 1430 6670

Key highlights of CERT-In guidelines

- Government entities are required to nominate a Chief Information Security Officer (CISO) and share the details with CERT-In. The roles and responsibilities of the CISO should be in-line with the requirements of MeitY[5].
- Cyber security and cyber resilience policies and procedures should be formulated in-line with this guideline.
- Internal audits should be conducted every six months or before and after the implementation or installation of major enhancements in the organisation.
- Follow-up audits should be conducted to ensure compliance and closure of vulnerabilities.
- Third-party security audits should be performed at least once a year.
- Compliance matrix checklist (included in Appendix I of the guideline) is required to be sent to nic.in, latest by the last Friday of every quarter.
- Cyber Crisis Management Plan (CCMP), including outlining the roles and responsibilities of organisational stakeholders within each central government ministry/department is required to be prepared and shared with CERT-In.

[5] https://www.meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf

Recommendations to help organisations comply with the guidelines

The guidelines issued by CERT-In includes specific security controls requirement incorporating leading practices in cybersecurity. Considering the dynamic threat landscape for government entities, the design and development of information security framework, and effective implementation of these guidelines will help organisations in protecting their "Crown Jewels",[6] and continually improving the cybersecurity ecosystem in the country.

The guidelines also incorporate requirements from previously published directions from CERT-In and MeitY for various areas. These directions include synching Network Time Protocol (NTP) servers with National Informatics Centre (NIC) services, following cloud security best practices published by MeitY, integrating websites and applications with the three National Single Sign-On (SSOs) for login purposes, and implementing Kavach multi-factor authentication (MFA) for NIC email accounts.

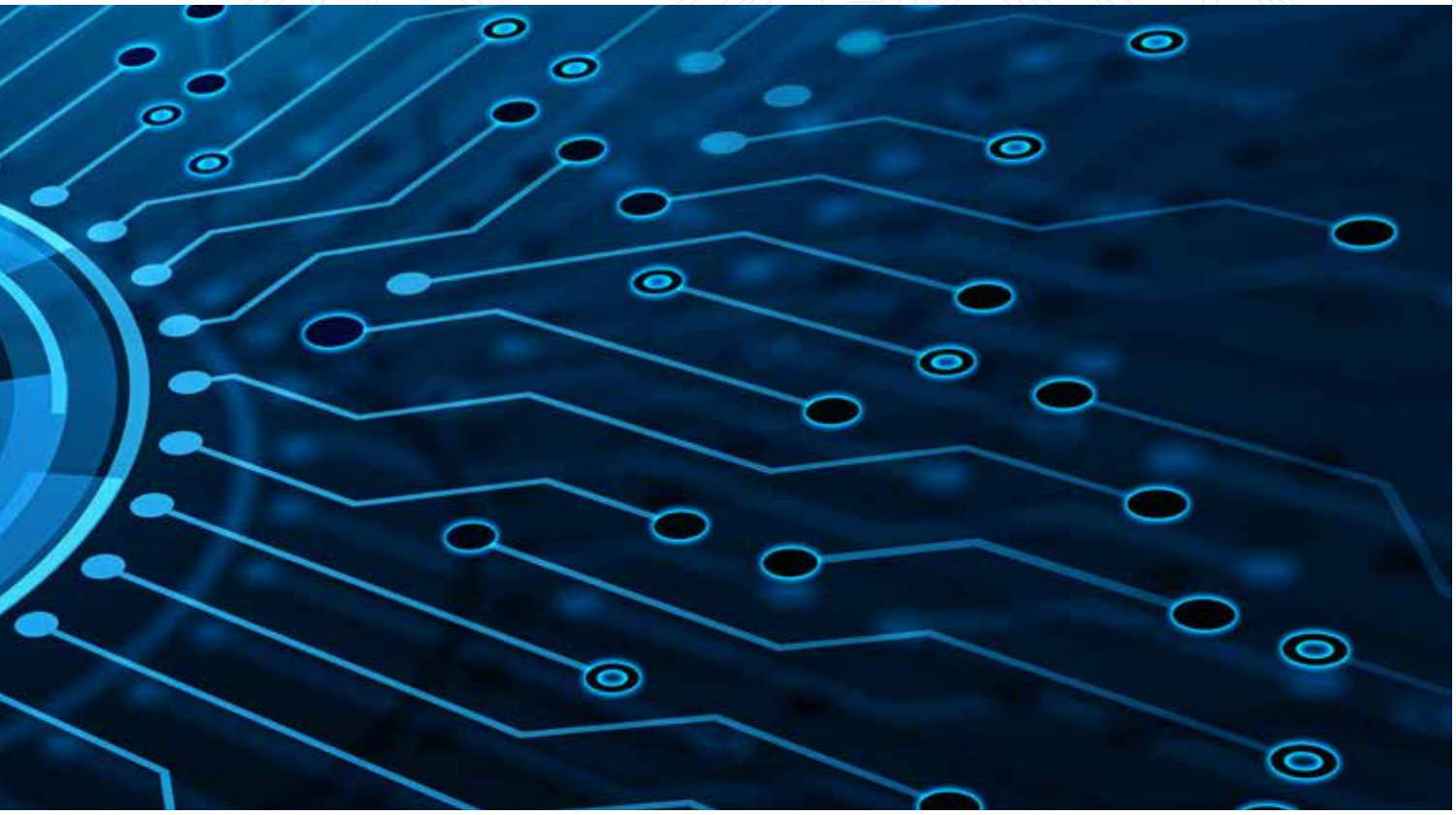
Government entities should develop a comprehensive approach to cyber-risk management in-line with these guidelines. The entities should also set up a strong governance framework for cybersecurity, comprising the senior management for steering the implementation and sustenance of the cybersecurity framework.

To achieve effective cyber risk management, the entities should identify their IT assets and classify them based on the impact to their Confidentiality (C), Integrity, (I) and Availability (A). Based on the classification, the Crown Jewels of the entity should be identified.

The emphasis should be given on user awareness and training, to help strengthen the "people link" in the defence chain. A focused and continuous effort should be placed to continuously monitor the threat landscape of the entity to help identify emerging threats and mitigate.

To measure the effectiveness of the controls metrics, such as Key Risk Indicators (KRIs), Key Control Indicators (KCIs) should be developed, assessed, and reported to the senior management regularly. Audits (internal, external, and third-party) should be conducted regularly per the guidelines, helping organisations measure compliance level with the requirements of the cybersecurity framework.

[6] Critical IT/OT assets, data of the government entity



The cybersecurity framework should be continually improved based on evolving threats, lessons learnt from past incidents, outcomes of the metric measurement, and audit findings.

Appoint a CISO and set up a cybersecurity steering committee.

Assess the current state of cybersecurity posture against the requirement of these guidelines.

Create a roadmap and allocate required budgets to implement the guidelines' requirements based on the gaps identified.

Design and develop or update the current cybersecurity framework (including policies, standards, and procedures) in-line with the requirements of these guidelines.

Implement and operationalise the cybersecurity framework.

Conduct regular awareness sessions and audits.

Include lessons learnt and continually improve the framework.

Conclusion

CERT-In has taken a comprehensive approach in detailing selective leading practices and processes required for standard cybersecurity coverage that extends beyond the existing boundaries (i.e., taking both internal and external ecosystems into consideration). This includes emerging cyber trends, such as securing social media, third parties (i.e., vendors) and cloud service adoption overlapped with regular audit assessments for a strengthened cybersecurity posture. Although these guidelines are specific to government entities, these serve as a reference guide or compliance check for enterprises, MSMEs, and the start-up sector embarking on their compliance journey. The emphasis on roles such as CISOs/CIOs and an appropriate cyber budget provides the much-needed support to IT teams, pushing for transformation in this domain.

Connect with us

Anthony Crasto
President, Risk Advisory
Deloitte India
acrasto@deloitte.com

Abhijit Katkar
Partner, Risk Advisory
Deloitte India
akatkar@deloitte.com

Tarun Kaura
Leader – Cyber Advisory,
Risk Advisory, Deloitte India
tkaura@deloitte.com

Digvijaysinh Chudasama
Partner, Risk Advisory
Deloitte India
dchudasama@deloitte.com

Vikas Garg
Partner, Risk Advisory
Deloitte India
vikasgarg@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
Deloitte India
deseshadri@deloitte.com

Contributor

K Deepak

Deloitte.