NATIONAL SECURITY COUNCIL SECRETARIAT

सत्यमेव जयते

CYBER SECURITY AUDIT BASELINE REQUIREMENTS

Abstract

This document provides the minimum-security assurance baseline expected across the Cyber Information Infrastructure of organisations and form the criterion for conduct of Cyber Security Audits.

Publication NSCS-46-16 Rev 1.0

October 2020

Inquiries regarding the use of this document are invited at:
National Cyber Security Coordinator
Sardar Patel Bhawan
Sansad Marg, New Delhi
India - 110001
ncss2020@gov.in

NATIONAL SECURITY COUNCIL SECRETARIAT
Publication NSCS 46-16 Rev 1.0
October 2020

सत्यमेव जयते

CYBER SECURITY AUDIT BASELINE REQUIREMENTS

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1. Introduction

The existence of an effective and appropriate supervision mechanism superimposed on minimum, common, and harmonised baselines, requirements, and measurement guidelines among the stakeholders is a pre-requisite for ensuring effective cyber security. While effective execution of this mechanism involves as a prerequisite extensive capability and capacity building amongst the stakeholders, there are some aspects that may be addressed based on common experiences and established best practices. This document is also not intended to discourage organizations from a risk management-based approach in favour of compliance-based approach.

Due to the relative heterogeneity of the various Information Technology sectors and technology dependent sectors, finding a minimum, common, and harmonised baselines is one of the primary and essential aspects. In this direction, based on inputs from various stakeholders in CERT-In, Ministry of Home Affairs, National Informatics Centre, National Critical Information Infrastructure Protection Centre and Defence Cyber Agency various category of baseline cyber security controls and the applicability of these markers has been identified and incorporated into this document. Based on the above, this document is being released to act as minimum-security assurance baseline expected across the cyber information infrastructure.

2. Objectives

The objective of Cyber Security Audit – Baseline Requirements (CSA-BR) for Cyber Information Infrastructure is to act as a minimum, common, and harmonised baseline criterion for cyber security audits.

3. Applicability

The document is intended to setup a common language for cyber security assessment across Government, Auditing organisations and Auditee organisations. It is will provide guidance to all organisations, the cyber security auditors, and the regulators of the sector of the organisation. It will be mandatorily applicable to owners and regulators of Critical Information Infrastructure of the nation including those responsible for ensuring its protection.

While the document is mandated to for all critical information infrastructure, all other public and private sector organisations are strongly encouraged to follow the baselines requirements. This will facilitate a stronger Cyber Security posture for all entities and ensure that the Cyber Security Audit process is more relevant, pragmatic, and functional to individual organization's threat landscape.

This is expected to be an evolving document and will be revised based on emerging threat landscape and contemporary acceptable best practices.

4. Roles and Responsibilities

(A) Auditee: -

(a) Prepare and present the Cyber Security Posture of the organization.

(b) Establish, maintain, and document the minimum internal controls as defined by Cyber Security Audit – Baseline Requirements (CSA-BR).

(c) Select and apply audit markers based on a realistic risk assessment.

(d) Identify and ensure the Organization complies with applicable laws and regulations.

(e) Assume management responsibility for the cyber security posture of the organization.

(f) Facilitate and enable the cyber security audit process.

(B) Auditor: -

(a) Maintain independence.

(b) Consider the organization's internal controls, understand them and take them into consideration as part of the audit process.

(c) Conduct the audit in accordance with auditing standards.

(d) Confirm the compliance of the organization to their own cyber security controls, best practices and the controls recommended by Cyber Security Audit – Baseline Requirements (CSA-BR).

5. Cyber Security Audits – Baseline Requirements

The Cyber Security Audit process is the procedural structure used by auditors to assess and evaluate the effectiveness of the IT organisation and how well it supports the organisation's overall goals and objectives.

Management needs to consider all the internal and external factors that affect auditing to determine the resources required to support these activities.

Cyber Security audit baseline is defined as the minimum controls to be audited for cyber security of an organisation. Baseline controls to be audited are grouped into following six categories: -

(a) Management

(b) Protection

(c) Detection

(d) Response

(e) Recovery

(f) Lessons Learnt & Improvements

The organisation along with the other stakeholders are expected to define the criticality of the asset based on the risk assessment conducted and accordingly define the exposure level of any given infrastructure along with the scope and granularity of the markers. The management is responsible for defining the risk appetite during this process and consequences thereof.

Section 7 contains baseline security controls to be implemented by the organisations for their cyber security infrastructure and to be audited against. Markers in table in Annexure-A are the evaluation area for the each of the cyber security controls, each uniquely identified by marker identifier.

6. Applicability of the Audit Markers

Organisation's Cyber Infrastructure is classified into three risk profiles. These risk profile classifications need to be done by the organisation themselves and as an outcome of risk assessment: -

(a) **High Risk Information Infrastructure**: Cyber-attack or disruption to cyber infrastructure will have impact on national security, public health & safety, economy, critical government operations or critical operations of the organisation.

(b) **Medium Risk Information Infrastructure**: Cyber-attack or disruption to cyber infrastructure will have impact limited within organisation and its dependencies but essential services of organisation will get affected.

(c) **Low Risk Information Infrastructure**: Cyber-attack or disruption to cyber infrastructure will have minimal impact on functions of the organisations.

The Audit Markers applicable to each of the 3 risk profiles are tabulated in the following tables 2, 3 and 4: -

(a) High Risk Information Infrastructure

Controls Categories	Mandatory Markers	Recommended Markers
Management	All Markers are Mandatory	Not Applicable
Protection	All Markers are Mandatory	Not Applicable
Detection	All Markers are Mandatory	Not Applicable
Response	All Markers are Mandatory	Not Applicable
Recovery	All Markers are Mandatory	Not Applicable
Lesson Learned & Improvements	All Markers are Mandatory	Not Applicable

Table 2: High Risk Information Infrastructure Audit Markers

(b) Medium Risk Information Infrastructure:

Controls Categories	Mandatory Markers	Recommended Markers
Management	All Markers are Mandatory	Not Applicable
Protection	All Markers are Mandatory except of Recommended Section	pro.12, pro.13, pro.20
Detection	All Markers are Mandatory except of Recommended Section	det.3
Response	All Markers are Mandatory except of Recommended Section	res.1, res.8
Recovery	All Markers are Mandatory	Not Applicable
Lesson Learned & Improvements	All Markers are Mandatory	Not Applicable

Table 3: Medium Risk Information Infrastructure Audit Markers

(c) Low Risk Information Infrastructure:

Controls Categories	Mandatory Markers	Recommended Markers
Management	All Markers are Mandatory except of Recommended Section	csm.11, csm.12, csm.14, csm.15
Protection	All Markers are Mandatory except of Recommended Section	pro.12, pro.13, pro.16, pro.20, pro.21
Detection	All Markers are Mandatory except of Recommended Section	det.3, det.4, det.7, det.9
Response	All Markers are Mandatory except of Recommended Section	res.1, res.8, res.9
Recovery	All Markers are Mandatory	Not Applicable
Lesson Learned & Improvements	All Markers are Mandatory except of Recommended Section	imp.4, imp.5

Table 4: Low Risk Information Infrastructure Audit Markers

7. Baseline Security Controls

(a) Management

Controls Categories	Markers	Marker Identifier
Management	Organisation Information Security Policy and Audit Process is defined and established	csm.1 *Cyber Security Management (csm)
	Frameworks, standards, and/or best practices are adopted for cyber security.	csm.2
	Commitment of Senior Management is ensured	csm.3
	Components of the infrastructure are identified and prioritised based on the criticality	csm.4
	Classification of Infrastructure as High, Medium and Low Risk is aligned to business process, classification affirmed during audit process	csm.5
	Components (Hardware, software, systems, applications, networking components) of the organisation information infrastructure are inventoried	csm.6
	Threats, Vulnerabilities, likelihoods, and impacts are identified	csm.7
	Cyber Security Risks are identified	csm.8
	Risk Management approach is effective and aligned to business process	csm.9
	Risk Treatment Plan is established and accepted/residual risks is in tune with criticality of related function	csm.10
	Critical Functions Continuity Plan /Business Continuity Plan is established	csm.11
	Critical Functions continuity Plan /Business Continuity Plan address resiliency of minimum-security controls are defined and implemented	csm.12

Controls Categories	Markers	Marker Identifier
Management	Information/cyber security roles & responsibilities are defined and informed and trained upon	csm.13
	Adequate manpower and resources for cyber security function is defined and provisioned	csm.14
	Cyber Security Crisis Management Plan is developed, implemented, and exercised upon by the organisation	csm.15
	Cyber security management approach addresses any legal, regulatory, sector specific compliance related to cyber security and same is adhered to by the organisation	csm.16
	Compliance to Audit Reports is ensured by the Management	csm.17
	Data is identified, labelled and its owner, custodians and users are made aware and responsible	csm.18
	Access Control - Administrative, Physical and Technical controls and their control model have been identified	csm.19

(b) Protection

Controls Categories	Markers	Marker Identifier
Protection	Physical security controls to critical assets are implemented and managed	pro.1 *Protective Controls (pro)
	Access control – Identified controls have been implemented in the specified model	pro.2
	Remote access and teleworking are controlled	pro.3
	Controls for Malware Protections are implemented and effectiveness is ensured.	pro.4

Controls Categories	Markers	Marker Identifier
Protection	Vulnerability and Patch Management process is implemented effectively	pro.5
	Controls for Removable media and BYOD/BYOT are implemented	pro.6
	Wireless network security controls are implemented	pro.7
	Secure configuration for hardware, software, Industrial control systems, network components and applications are implemented and managed	pro.8
	Secure software development lifecycle is ensured (in-house as well as outsourced)	pro.9
	Perimeter security devices like Firewall, IDS/IPS, network monitoring, etc. are deployed in the organization and they are monitored on continuous basis.	pro.10
	Vulnerability Assessment (VA) and implementation of corrective actions are done by the organization on continuous basis (VA by internal team as well as empanelled Third-Party)	pro.11
	Defining scope of Penetration Testing Exercises and ensuring its periodic conduct	pro.12
	Periodic Participation of organisation in national/ sectoral/ organisational Cyber Security Exercises	pro.13
	Role based Cyber security Training and awareness programs are conducted periodically for all employee and associated external entities	pro.14
	Content of cyber security trainings is appropriate	pro.15

Controls Categories	Markers	Marker Identifier
Protection	BCP and Disaster management plan are tested periodically and continuity of security controls is tested.	pro.16
	Data protection (-in-transit, -at-rest) controls are implemented effectively	pro.17
	Data retention and destruction policies are defined and implemented	pro.18
	Change Control policy and practices are defined and implemented	pro.19
	Mapping and Securing Supply Chain including baseline compliance by vendors	pro.20
	Secure Disposal of IT Equipment	pro.21

(c) Detection

Controls Categories	Markers	Marker Identifier
Detection	Scope, mechanism, and frequency of log collection defined and implemented	det.1 *Detection Controls (det)
	Mechanisms for regularly analysing the alert/log data collected from different security devices	det.2
	Daily Log analysis of the critical services	det.3
	Monitoring of accounts and access is implemented	det.4
	Network Monitoring is implemented	det.5
	Physical security controls are monitored for possible cyber security incidents	det.6

Controls Categories	Markers	Marker Identifier
Detection	Adequate resources for log and alert analysis are available and role & responsibilities are clearly defined	det.7
	Synchronisation with singular time source	det.8
	Detected incidents are analysed technically to determine cause, impact, attacker methodology	det.9

(d) Response

Controls Categories	Markers	Marker Identifier
Response	Cyber Crisis Management Plan in line with National Cyber Crisis Management Plan is prepared and established.	res.1 *Incident Response (res)
	Incident Response Plan is implemented	res.2
	Roles and responsibilities for Incident Response are clearly defined.	res.3
	Incident Escalation matrix is defined.	res.4
	Communication mechanism within Organisation is clearly defined for incident resolution	res.5
	Communication mechanism with stakeholders and agencies is clearly defined for incident resolution	res.6
	Contact details of Ministries, stakeholders, vendors and agencies like NCIIPC & CERT-In for incident resolutions are up to date and documented	res.7
	Incident/abuse reporting channel and mechanism is defined and implemented	res.8

Controls Categories	Markers	Marker Identifier
Response	Information sharing mechanism with external entities are clearly defined and implemented	res.9
	Incidents are recorded and investigated in terms of impact, vulnerability exploited or attempted to exploit, attacker methodology and attack source	res.10
	Incidents are contained and mitigated	res.11

(e) Recovery

Controls Categories	Markers	Marker Identifier
Recovery	Recovery Plan is defined and implemented	rec.1 *Recovery Controls (rec)
	Resources are available for recovery of critical functions	rec.2
	Recovery plan incorporate lesson learned from crisis/incident	rec.3

(f) Lesson Learnt & Improvements

Controls Categories	Markers	Marker Identifier
Lesson Learnt & Improvements	Lesson Learnt from incidents and cyber exercises are incorporated in response plan	imp.1 *Improvement (imp)
	Lesson learnt and improvement plans are documented and commitment of management is ensured	imp.2

Controls Categories	Markers	Marker Identifier
	CCMP and incident handling procedures/response plan are improved and updated	imp.3
	Organisation cyber security posture is improved as compared to last reference point (last assessment, last year, etc.)	imp.4
	Organisation performance improved in successive cyber security exercises and trainings	imp.5

ACRONYMS

BCP	Business Continuity Plan
BYOD	Bring Your Own Device
BYOT	Bring Your Own Technology
CCMP	Cyber Crisis Management Plan
CII	Critical Information Infrastructure
CSA-BR	Cyber Security Audit – Baseline Requirements
csm	Cyber Security Management
det	Detection Controls
IDS	Intrusion Detection Systems
imp	Improvement
IPS	Intrusion Protection System
IT	Information Technology
pro	Protective Controls
rec	Recovery Controls
res	Incident Response
VA	Vulnerability Analysis

Notes