NATIONAL CRITICAL INFORMATION INFRASTRUCTURE PROTECTION CENTRE

STANDARD OPERATING PROCEDURE
(SOP)

Auditing of CIIs/Protected Systems by Private/Government Organisation

June 2017

NCIIPC, Block-III, Old JNU Campus
New Delhi-110067

Table of Contents

Abbreviations

CERT-In	Computer Emergency Response Team - India
CI	Critical Infrastructure
CII	Critical Information Infrastructure
ISMS	Information Security Management System
IT	Information Technology
MHA	Ministry of Home Affairs
NDA	Non-Disclosure Agreement
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
SOP	Standard Operating Procedure
STQC	Standardisation Testing and Quality Control

1. Introduction

1.1. As per gazette notification on 16th Jan 2014, following duties with respect to auditing Critical Information Infrastructure (CII) have to be performed by NCIIPC:-

1.1.1. “Evolving protection strategies, policies, vulnerability assessment and auditing methodologies and plans for their dissemination and implementation for protection of Critical Information Infrastructure”

1.1.2. “Developing or organising training and awareness programs as also nurturing and development of audit and certification agencies for protection of Critical Information Infrastructure”

1.2. Various global standards and guidelines exist to define and operate Information Security Management Systems (ISMS). These standards have been adapted by industry to achieve an efficient Information Security Infrastructure. Some of the standards like ISO27001 ISMS, NERC-CIP etc have received recognition and acceptance by the industry including elements of our CII in the last few years.

1.3. CERT-in has empanelled a list of auditors for conducting Cyber Security Audit in India. Guidelines and framework on Information Security Audit have also been released by RBI and SEBI. NCIIPC has released a document on “Guidelines for the Protection of National Critical Information version 2.0” in 2015. This document specifies families of controls that may be appropriate for an organisation during various phases of business processes.

1.4. As part of policy, many organisations are conducting cyber security audit for their IT infrastructure on a regular basis. Considering the importance of cyber security framework and their proper implementation in a Critical Information Infrastructure, there is a need to define a Standard Operating Procedure for effective implementation of cyber security all over CII/Protected system without compromising national safety and security.

2. Definitions

2.1. **Cyber Security Audit:** A Cyber Security Audit is the systematic technical assessment of an IT infrastructure on the baseline of an Information Security standards or the information security policy of the organisation.

2.2. **Critical Information Infrastructure (CII):** As per IT act of India, Critical Information Infrastructure is any computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

2.3. **Protected System**: A Protected System is the IT infrastructure of an organisation that has been recognised and notified by Gazette of India as Critical Information Infrastructure.

3. Objective

Present document specifies Standard Operating Procedure (SOP) to define guidelines as to which Critical Infrastructure (CI) can be audited by private organisations and which must be audited by Govt. bodies such as STQC based on their strategic importance.

4. Scope of SOP

4.1. This standard operating procedure is applicable for all Critical Information Infrastructures in India, which have been identified or in the process of notification or have been notified as Protected Systems.

4.2. While referring this document, it must be understood that every critical sector organisations may contain critical as well as non-critical network segments in their IT infrastructure. The organisations have to make decisions on what to audit and how to audit their IT infrastructure.

5. Challenges

5.1. Adequate access and information has to be shared with the auditor to conduct an efficient Cyber security audit. Some factors that could lead to possible conflict of interest are:-

5.1.1. Possibledilution ofNon-Disclosure Agreement (NDA) with auditors.

5.1.2. Audit details captured during Information Security audit including all vulnerabilities and gaps of various organisations are typically retained by an auditing organisation for reasonable period (may be 2-3 years) in order to address any queries raised by auditee.

5.1.3. Compliance with the legal, regulatory (for example, ensuring protection of official secret acts) and safeguarding national security data may be at risk depending upon who the auditors are.

5.2. The above are indicative concerns with respect to the level of trust and control that a CII/Protected System may establish with an auditor during or after conduct of a cyber security audit.

6. Audit Criteria

6.1. Based on MHA guidelines on classification of Information (Reference: Manual on paper records Issued by Ministry of Home Affairs, 1994), network segments in an IT infrastructure can also be classified in similar fashion. The classification of network segments considering the type of information used within, can be classified as follows:-

6.1.1. **Top Secret:** Information, unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for nation's closest secrets and is to be used with great reserve.

6.1.2. **Secret**: Information, unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information.

6.1.3. **Confidential**: Information, unauthorized disclosure of which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization, or could affect the organization in its functioning.

6.1.4. **Restricted**: Information, which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose

6.1.5. **Unclassified**: Information that requires no protection against disclosure e.g. Public releases.

6.2. Depending on presence of various information classification as defined above, network segments in a CII/Protected Systems can be categorised into following two categories:-

6.2.1. **Critical Segment Category-I**

6.2.1.1. Network segments in a CII/Protected System with classification “Secret” or “Top Secret” would fall under this category.

6.2.1.2. Cyber security audit of a “Critical Segment Category-I” must be carried out by a Government auditor. The auditors must be working as a permanent employee in a Government organisation and they must have served at least 4 years for Government of India.

6.2.2. **Critical Segment Category-II**

6.2.2.1. Network segments in a CII/Protected System with classification not greater than “Confidential” would fall under this category.

6.2.2.2. Cyber security audit of a “Critical Segment Category-II” may be carried out by a private auditor.

7. Auditor Selection

7.1. Private/Government Auditors selected for auditing CII/Protected Systems (includingCritical Segment Category-I andCritical Segment Category-II) must meet the following requirements:-

7.1.1. They must have minimum 6 years of experience in cyber security audit.

7.1.2. They must have experience of conducting cyber security audit of at least 10 organisations.

7.1.3. Auditors with experience in cyber security audit of CII/protected system may be given weightage.

7.1.4. There must not be any complaint against the external auditors by any CII/protected system.

7.2. Government auditors like STQC or any othergovernment agency empanelled by CERT-in may be considered for conducting audit of “Critical Segment Category-I”.

8. Types of Audit

Depending on the selection of auditors, audit may be divided into three different types as described below:-

8.1. **Internal Audit**

8.1.1. An internal audit is carried out by Information Security team of the organisation who are part of the Information Security Group within the organisation.

8.1.2. The members of an internal audit team must be a group of people with working knowledge of Information Security and operational technology used within the organisation. They must not be a part of the operational team.

8.2. **External Audit**

8.2.1. An external party audit can be carried out by any of the private/public auditors empanelled by Govt of India and/or recognised by popular international standards as recognised by Govt of India such as ISO27001, National Information Security Policy and Guidelines etc.

8.2.2. In case, the external auditors happen to be the implementer of any component or complete IT infrastructure of the auditee organisation, then they may be referred as second party. Otherwise, external auditor may be referred as third party.

8.3. **Special Audit**

8.3.1. Specially formed group of auditors chosen from various government establishment for carrying out an audit of a CII/Protected System on a special requirement.

8.3.2. The group of auditors may be chosen from the pool of auditors available in the Information Security Group of various CIIs/Protected Systems.

8.3.3. This group may be constituted by picking expertise from various Govt establishments considering the types of technologies to be audited.

8.3.4. Any group member of a special audit team shall not be chosen from the CII/protected system being audited, to ensure a transparent and fair audit.

8.3.5. Indicative conditions for special audits are listed below:-

8.3.5.1. Effectiveness of ISMS in a CII/Protected system is doubtable.

8.3.5.2. Request from the top management of a CII/Protected system to carry out special audit for them.

9. Audit Process

Every organisations in a critical sector must identify the networks and classify its segments as per classification criteria defined in Para 6.2. Non-Disclosure Agreement between auditor and auditee organization must be signed and enforceable as per Court of Law. Compliance/Closure of audit observations must be reported within two months. The report shall be prepared in the format as defined in "Cyber Security Assessment Framework" of CERT-In. Non-compliance and resultant residual risk must be signed off by the higher management within two months of completion of audit. Once the Category-I and Category-II critical network segments have been identified by the CIIs/Protected System owner, following audit processes must be exercised:-

9.1. Every CII/Protected System must form an Internal Audit team as part of the Information Security Group within the organisation. This group shall be responsible for oversight of Information Security within the CII/Protected system. The internal audit teammust conduct an internal cyber security audit every half yearly.

9.2. Every CII/Protected System shall carry out an external audit by a private or government auditor, based on the audit criteria as define in Para6. The CII/Protected system shall plan for an external audit in following terms:-

9.2.1. An external cyber security audit must be performed on annual basis or whenever there is upgradation/change in IT infrastructure/application/system software.

9.2.2. Any three successive audits shall not be carried out by the same external auditor.

9.3. A special audit shall be carried out in case of a specific requirements as defined in Para 8.3.5. A special audit will be carried out either on consideration of a request from a CII/Protected System or initiation by NCIIPC. Following tasks with specified deadlines shall be carried out by the special audit team (all deadlines are with reference to the date of approval for undertaking a special cyber security audit):-

9.3.1. NCIIPC shall obtain relevant information required to carry out the Cyber Security Audit from CII/Protected system within two weeks.

9.3.2. Audit team shall be constituted within 3 weeks.

9.3.3. The audit team will meet and agree upon an audit plan for the CII/Protected System.

9.3.4. The team shall carry out the audit as per the scheduled plan in coordination with the CII/Protected system. This shall not exceed a period more than 6 months.

9.4. Information / details captured during audit must not be retained beyond six months.

9.5. High level secrecy must be insured for the safeguarding of national security data / secret data which can be accessed by the authorised users. Such data can be shared with the audit team only after the approval of the Head of the Organisation / Designated Authority considering the requirements for the audit and types of the auditor i.e. Government or private auditor.

10. Review

Present SOP shall be reviewed whenever there is a requirement of an update.