PROFESSIONAL PROGRAMME

UPDATES FOR INFORMATION TECHNOLOGY AND SYSTEMS AUDIT

(Relevant for students appearing in December, 2018 examination)

MODULE 2 PAPER 4

Disclaimer:

This document has been prepared purely for academic purposes only and it does not necessarily reflect the views of ICSI. Any person wishing to act on the basis of this document should do so only after cross checking with the original source.

Students appearing in December 2018 Examination shall note the following:

Students are also required to update themselves on all the relevant Notifications, Circulars, Clarifications, etc. issued by the Competent Authorities to relate to Law covering Information Technology and Systems Audit & Central Government on or before six months prior to the date of the examination.

These Updates are to facilitate the students to acquaint themselves with the amendments in laws relating to Information Technology and System Audit upto June, 2018, applicable for December, 2018 Examination. The students are advised to read their Study Material (2016 Edition) along with these Updates. In the event of any doubt, students may write to the Institute for clarifications at academics@icsi.edu

Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018[1]

The Ministry of Electronics and Information Technology (MEITY) vide notification dated 22nd May, 2018 has notified the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 ("Rules") which shall come into force on the date of publication in the Official Gazette.

The Rules detail the responsibilities to be met by various organisations which have a protected system. "**Protected System**" means any computer, computer system or computer network of any organisations notified under section 70 of the Act, in the official gazette by appropriate Government.[2]

What is a Protected System

According to the Rules a Protected System is any computer, computer system or computer network of any Organization as notified under Section 70 of the Information Technology Act, 2000, in the official gazette by the appropriate Government.[3]

Constitution of Information Security Steering Committee

The Rules mandate that an organisation having a Protected System shall constitute an **Information Security Steering Committee** (ISSC) whose chairman shall be the Chief Executive Officer/ Managing Director/ Secretary of the organisation (Rule 3 (1) (a)). The composition of the ISSC as mentioned Rule 3 (1) (b) shall be as follows:

- IT Head or equivalent;
- Chief Information Security Officer (CISO);
- Financial Advisor or equivalent;
- Representative of National Critical Information Infrastructure Protection Centre (NCIIPC);
- Any other expert(s) to be nominated by the organisation.

[1] Available at: http://meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf
[2] See, https://novojuris.com/2018/08/24/regulatory-update-ministry-of-electronics-and-information-technology-information-technology-information-security-practices-and-procedures-for-protected-system-rules-2018/
[3] See, http://www.mondaq.com/india/x/730070/Security/Information+Technology+Information+Security+Practices+And+Procedures+For+Protected+System+Rules+2018+Notified

Roles and Responsibilities of the Information Security Steering Committee

The Rules prescribe the vital roles and responsibilities of the Information Security Steering Committee the significant ones of which are as follows: -

- To approve all the Information Security Policies of the 'Protected System' any significant changes in network configuration impacting the "Protected System" or any significant change in application of the "Protected System".
- To establish mechanism for timely communication of cyber incident(s) related to "Protected System" to Information Security Steering Committee. A detailed definition as to what comprises of a cyber incident is mentioned in the Rules as an adverse incident that may result in impairing the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorization or threaten interests of public at large.
- To establish mechanism for sharing of results of all information security audits and compliance of "Protected System" to Information Security Steering Committee.
- To assess validation of "Protected System" after every two years.

The Rules prescribe certain mandatory practices and infrastructural compliances to be followed by any organization having a Protected System.

The ISSC shall be the apex body and its responsibilities (as mentioned under Rule 3(2)) shall be as follows:

- All the information security policies of a Protected System has to be approved by the ISSC.
- Any significant change in the network configuration which has an impact on the Protected System shall be approved by ISSC.
- It is mandatory that each significant change in the application(s) of the Protected System shall be approved by ISSC.
- A mechanism has to be established which ensures timely communication of the cyber incident(s) related to Protected System to the ISSC.
- Protected System shall be validated for assessment after every 2 (two) years.

The Rules also lay down certain roles and responsibilities for the organisations having a Protected System (as mentioned under Rule 3(3)).

Some of the key responsibilities are as follows:

- Nominate an officer as CISO whose roles and responsibilities shall be as per the latest Guidelines for Protection of Critical Information Infrastructure ("**Guidelines**") and "Roles and Responsibilities of CISOs of Critical Sectors in India" released by the (NCIIPC);
- Plan, establish, implement, operate, monitor, review, maintain and continually improve **Information Security Management System** (ISMS) of its system as per the latest Guidelines released by the NCIIPC or an industry accepted standard duly approved by the said NCIIPC;
- Ensure that the network architecture of Protected System shall be documented;
- The same shall be reviewed at least once a year, or whenever required, or according to the (ISMS);
- Plan, develop, maintain and review the documents of **inventory of hardware and software** related to Protected System;
- Ensure that the **vulnerability/threat/risk (V/T/R) analysis** for the cyber security architecture of Protected System shall be carried out at least once a year. Further the (V/T/R) analysis shall be initiated whenever there is significant change or upgrade in the system, by intimation of the same to ISSC;
- Plan, establish, implement, operate, monitor, review, **and continually improve Cyber Crisis** Management Plan (CCMP) in close coordination with NCIIPC;
- Ensure conduct of internal and external Information Security audits periodically.
- Establish a **Cyber Security Operation Center (C-SOC)** using such tools and technologies to implement preventive, detective and corrective controls to secure against advanced and emerging cyber threats.
- The records of unauthorised access, unusual and malicious activity, if any, shall be documented;
- Establish a **Network Operation Center (NOC)** using tools and techniques to manage control and monitor the network(s) of Protected System.

- Plan, develop, maintain and review the process of taking regular backup of logs of networking devices, perimeter devices, etc. and services supporting "Protected System" and the logs shall be handled as per the ISMS as suggested.

The Rules also lay down responsibilities of the CISO towards NCIIPC (As mentioned under Rule 4). They are as follows:

- CISO shall maintain regular contact with the NCIIPC and will be responsible for implementing the security measures.
- CISO shall share inform the NCIIPC, whenever there is any change, and incorporate the inputs/feedbacks suggested by the said (NCIIPC)- with regard to details of Critical Information Infrastructure (CII), details of ISSC, network architecture of the Protected System., etc.
- CISO shall establish a process, in consultation with the NCIIPC, for sharing of logs of "Protected System" with NCIIPC to help detect anomalies and generate threat intelligence on real time basis.
- CISO shall also establish a process of sharing documented records of Cyber Security Operation Center (related to unauthorised access, unusual and malicious activity) of Protected System with NCIIPC to facilitate issue of guidelines, advisories and vulnerability, audit notes etc. relating to Protected System.
- CISO shall establish a process in consultation with NCIIPC, for timely communication of cyber incident(s) on Protected System to the said NCIIPC.