

Name : Alok Bhawankar

Div : CSE Final Year B.Tech

Subject : ISM

PRN : 1032170126

Theory Assignment 2

Q1) Define ISO 27001, what is its role in ISMS?

=> ISO 27001 is "ISO/IEC 27001 - Information technology - Security techniques - Information security Management requirements".

- It is an ISO standard published by International Organization for Standardization (ISO) and

- International electrotechnical commission (IEC)

- ISO 27001 was developed to help organizations of all scales to protect their information in systematic and cost effective manner. It sets a bare minimum for Information Security in any organization.

- Along with bare minimum and basic idea for protecting valuable information, a company can also be ISO 27001 certified and prove to its stakeholders that it protects their data.

- Basic aim of 27001 is to protect three aspects of information

- => Confidentiality

- => Integrity

- => Availability

★ Role of ISO 27001 in ISMS

- Compliance with legal requirements - ISO 27001 gives a perfect means to comply with most of the legal requirements
- Low cost - The cost of getting ISO standardised is low than the long-term saving achieved. It helps in preventing incidents from happening.
- Resolution of processes - ISO 27001 encourages companies to write down their main processes
- Protect confidentiality, integrity and availability of information.
- Manage and mitigate risk - Lays a process for the same.

Q2. write a brief on PDCA

⇒ PDCA or Plan Do check act is a model for carrying out change. For continuous improvement of a system PDCA cycle has to be repeated again and again.

→ Usage of PDCA cycle comes in the following situation

- Starting a new improvement project
- Development of improved design, product or service
- Implementation of change
- Continuous improvement
- Prioritizing problems for resolution

→ PDCA procedure

1. Plan: Recognizing an opportunity for change or improvement. Requires means to measure effectiveness of change expected improvements and target. Relevant metrics can be used.
2. Do: Making the intended change and carry out some study.
3. Check: Measure effects of changes, analyze results and identify what you have learned.
4. Act: The outcome of the check step determines the next course of action. If the change is successful, incorporate changes. Update the metrics and set them as baseline for future improvements.

Q 3) What is NIST 800? How NIST compliance is done?

- ⇒ The NIST 800 Series is a set of documents that establish United States Federal Government computer security policies, procedures and guidelines.
- NIST documents are available free of charge and can be useful for business, educational institutions and government agencies.
 - These publications cover recommended procedures and criteria for assessing and documenting threats and vulnerabilities and implementing controls, risk mitigation and security measures.

→ Compliance

• NIST outlines steps towards FISMA compliance:

- 1) Categorize the data and information you need to protect
- 2) Baseline development for protecting information
- 3) Conduct risk assessments to refine baseline controls.
- 4) Document baseline controls in a security plan.
- 5) Roll out security controls to your information systems
- 6) Monitor performance to measure the efficacy of security controls.
- 7) Find agency level risk based on assessment
- 8) Authorize the information system for processing
- 9) Continuously monitor security controls

Q4) Write a short note on Digital Signature E-governance?

→ Digital Signature:-

- Digital Signature is an advanced technique used to authenticate the sender, maintain integrity of information in the form of message, software or digital document.
- They are unique to each signer.
- They follow a protocol called Public Key Infrastructure (PKI). The digital signature solution provider uses a mathematical algorithm to generate public and private keys.

- The Act purports to facilitate electronic trade and commerce eliminate barriers and obstacles coming in the way of e-commerce.
- A chapter in the IT Act talks about various offences and the investigation of said offences.