Name: Alok Bhawankar

Div: CSE Final Year B. Tech

Subject: ISM

PRN: 1032170126

Theory Assignment 2

GI) Define Iso27001 what is its role in Isms?

=) Iso 27003 is "Iso/IEC 27001 - Information
technology - Security techniques - Information
security Management requirements"

It is an Iso standard published by Internation
Orginization for Standard published by Internation
Orginization for Standard Commission (IEC)

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

Along with bare minimum and basic idea for
protecting valuable information, a company con
also be Iso27001 certified and prove to its
stakeholders had it protects their data.

Basic aim of 2.7001 is 10 protect three aspects of information

=) can Fidentiality

-> Integrity

=) Availability

* Role Of JSO 27001 in JSMS · compliance with legal requirements - \$50 27001
gives a perfect mans to comply with most of the
legal requirements legal requirements Low cost - the cost of getting Iso standistised is low than he long-term saving achieved. gt helps in preventing inlidents from happening.

Resolution of processes - Iso 2000 en courages

eompanies 16 write down their main processes

protect confidentiality, integrity and availability of information. manage and mitigat risk - lays a process for the same.

92. 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 rejected again on a again.

Usage of PDCA cyck comes in the following

Situation Starting a new improvement project Development of improved dosign, product or service

Implementation of change

Continuous improvement Prioritizing problems for sesolution

PDCA procedure

I. Plan: Recognizing an opportunity for change
or improvement. Requires means to measure
effectionness of change expected improvements
and target. Relevant metries can be used.

2 Do: Making the intented change and corry
out some study.

3 Check: Measure effects of changes, analyze
results and identity what you have learned.

4 Act: The outcome of the check step determines
the next ourse of action of the change is
Successful in corporate changes - update the
metrics and set them as baseline for future
improvements.

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

The NJST 800 series is a set of documents

That establish united states Federal government

computer security policies, procedure and guideling

NJST 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

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 to protect controls. 5) Rolls out security controls to your information sustems Systems

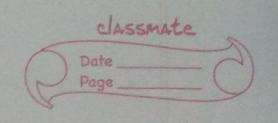
G) Monitor performance to measure the efficacy

at security controls.

7) Find agency level risk based on assessment

8) Kushorize the information system for processing.

9) Con lin vously monitor security controls. E-governance? Digital Signature F-governance? =) Digital Signature:to authoricate 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 Intrastructure CPKI) The Digital signature to generate public and private vegs



and commerce aliminate barriers and obstacles coming in the way of e-commerce.

Achapter in the IT Act talks about various offences and the investigation of said offences