CS 205 Mid term short notes for Sprimng 2023

Made By Muhammad Qasim Ali For any Query 03337435091

What is Cyber Security?

– Precautions taken to guard against unauthorized access to data (in electronic form) or information Systems connected to the internet

1. Information security by SANS define

Ans: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

2. Transformation model layers

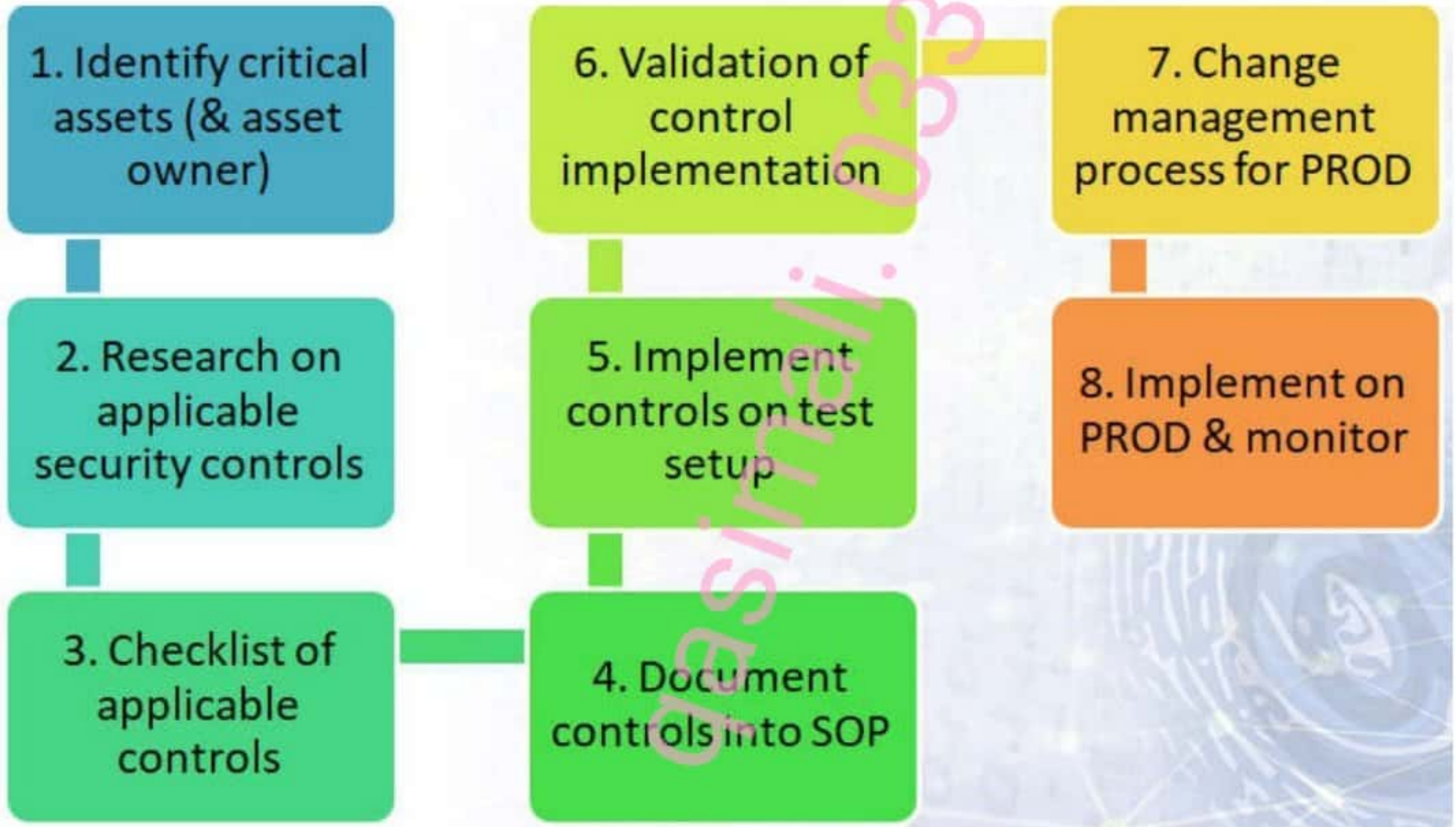
Ans:

1. Security hardening
2. Vulnerability management
3. Security engineering
4. Security governance

3. Eight (8) step methodology

Ans:

8 STEP SECURITY HARDENING METHODOLOGY



4. **Write any five steps in information security program**

Ans:

- Assessing security risks and gaps
- Implementing security controls
- Monitoring, measurement, & analysis
- Management reviews and internal audit

Accreditation/testing

5. **Who Are The Players In Information Security?**

- Government
- Industry & sectors
- International organizations
- Professional associations
- Academia and research organizations
- Vendors and suppliers

6. **SSh protocols versions names**

Description:
SSH supports 2 different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol & was subject to security issues. SSH2 is more advanced and secure.

- Rationale: SSH v1 suffers from insecurities that do not affect SSH v2.

7. **Security challenges in Box security mention any two**

Ans:

"Box Security" refers to a prevalent approach in the industry, especially in larger organizations in which
the solution for every security challenge is in the form of a "box" or device

- **Box for :**

- Email security
- Web security
- FW

- IPS
- APT attack prevention
- DDOS prevention
- Network DLP
- Network Forensics
- Others

What is a disaster?

– Any significant event that causes disruption of information technology processing facilities, thus affecting the operations of the business.

• **What is disaster recovery (DR)?**

- DR is an area of security that allows an organization to maintain or quickly resume mission critical (IT) functions following a disaster

• Three Pillars of Information Security:

- **Confidentiality**: keeping information secret
- **Integrity**: keeping information in its original form
- **Availability:** keeping information and information systems available for use

Three pillars of information security Implemention: (yeh implementation hai)

- People
- Process
- Technology

CIS 20 Controls:

First 5 CIS Controls
Eliminate the vast majority of your organisation's vulnerabilities

1: **Inventory of Authorized and Unauthorized Devices**
2: **Inventory of Authorized and Unauthorized Software**
3: **Secure Configurations for Hardware and Software**
4: **Continuous Vulnerability Assessment and Remediation**
5: **Controlled Use of Administrative Privileges**

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: **Maintenance, Monitoring, and Analysis of Audit Logs**
7: **Email and Web Browser Protections**
8: **Malware Defenses**
9: **Limitation and Control of Network Ports**
10: **Data Recovery Capability**
11: **Secure Configurations for Network Devices**
12: **Boundary Defense**
13: **Data Protection**
14: **Controlled Access Based on the Need to Know**
15: **Wireless Access Control**
16: **Account Monitoring and Control**
17: **Security Skills Assessment and Appropriate Training to Fill Gaps**
18: **Application Software Security**
19: **Incident Response and Management**
20: **Penetration Tests and Red Team Exercises**

Digital world Vu u tube chanel

You tube chanel for more videos DIGITAL WORLD VU

CIS Benchmark name. (Which has minimum or max remember its count number)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	**107**

CIS benchmark in profile applicability

- Profile applicability (ASA 8.X, ASA 9.X)
- Description
- Rationale
- Audit
- Remediation
- Default value
- References

Disa STIG component/content names

STIG content:

- General information (title)
- Discussion
- Check content
- Fix text

- CCI (References)

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

CCI (Control Correlation Identifier) (for Mcqz only. CCi stands for ?)

OWASP Software Assurance Maturity Model (SAMM) **Governance Phase:**

– Strategy & Metrics
- Education & Guidance
- Policy & Compliance

OWASP Software Assurance Maturity Model (SAMM) **Construction Phase:**

- Security Requirements
- Threat Assessment

Secure Architecture

What is business continuity? (BC.)

– Business Continuity (BC) is the capability of the org to continue delivery of products or services
at acceptable predefined levels following a disruptive incident

Bangladesh Bank SWIFT Hack – Feb 2016: Hackers used SWIFT credentials of Bangladesh Central
Bank employees to send more than three dozen fraudulent money transfer requests.
– Requests sent to the Federal Reserve Bank of New York asking the bank to transfer millions of the Bangladesh Bank's funds to bank accounts in the Philippines, Sri Lanka and other parts of Asia.
– USD 81 million stolen
– Total impact could have been USD 1 billion

Ransomware attack hits 99 countries with UK hospitals among targets – live updates

What is the function of active directory in an enterprise network?

Active Directory is a directory service by Microsoft that provides centralized management and authentication for users, computers, and resources in an enterprise network, facilitating secure access and efficient administration.

How web and email can secured against malware and attacks in enterprise.

To secure web and email in an enterprise, implement antivirus software, firewalls, and intrusion detection systems. Train employees on security best practices, use email encryption, update software, employ MFA, monitor traffic, backup data, and conduct security assessments.

Software security flow?

Software security flow refers to the systematic process of identifying, assessing, and mitigating security risks and vulnerabilities in software applications, following a structured approach to ensure the development of secure and robust software systems.

What is an IT asset?

– An IT asset is any resource such as hardware, software, information, human owned or utilized by the organization for IT processing

)

Typical security tools used in an enterprise:

- Enterprise antivirus
- MS Active Directory (AD)
- Vulnerability manager
- Logs management
- Network & performance monitoring

Automated backups

Topic No 25: Major Components: Enterprise IT Network

- Edge router
- NGN FW
- DMZ:
- IPS & N-DLP
- Distribution switch
- Data center switch & FW
- Access switch
- NAC
- SOC:

– SIEM
– VM

- System AV
- Server HIPS
- UTM
- Mobile device – MDM

- **Backup considerations:**

– What to backup?
– Backup location?
– Freq of backup?
– Backup operator?
– Backup checker (verification)?
– Backup test & security methods?
– Technology & tools used for backup?