Prepared By M.Qasim Ali
03337435091

01 : SECURITY HARDENING – SOFTWARE APPLICATIONS SOFTWARE SECURITY WORKFLOW ? (Most Repeated question)

1. Research Security Controls
2. 2. Apply Security Controls (Hardening)
3. 3. Code Review & Automated Testing (Validation)
4. 4. Harden Server Environment
5. 5. Pen Test & Accreditation (Move to PROD)

Q No3: Common challenges with box security?

1: Other challenges with "box security" approach: –

2: Shortage of staff (IT & security)

3: Training and skill required to operate the sophisticated devices and features

Question No 03: CIS and DISA compression?

Prepared By M.Qasim Ali
03337435091

01 : SECURITY HARDENING – SOFTWARE APPLICATIONS SOFTWARE SECURITY WORKFLOW ? (Most Repeated question)

1. Research Security Controls
2. 2. Apply Security Controls (Hardening)
3. 3. Code Review & Automated Testing (Validation)
4. 4. Harden Server Environment
5. 5. Pen Test & Accreditation (Move to PROD)

Q No3: Common challenges with box security?

1: Other challenges with “box security” approach: –

2: Shortage of staff (IT & security)

3: Training and skill required to operate the sophisticated devices and features

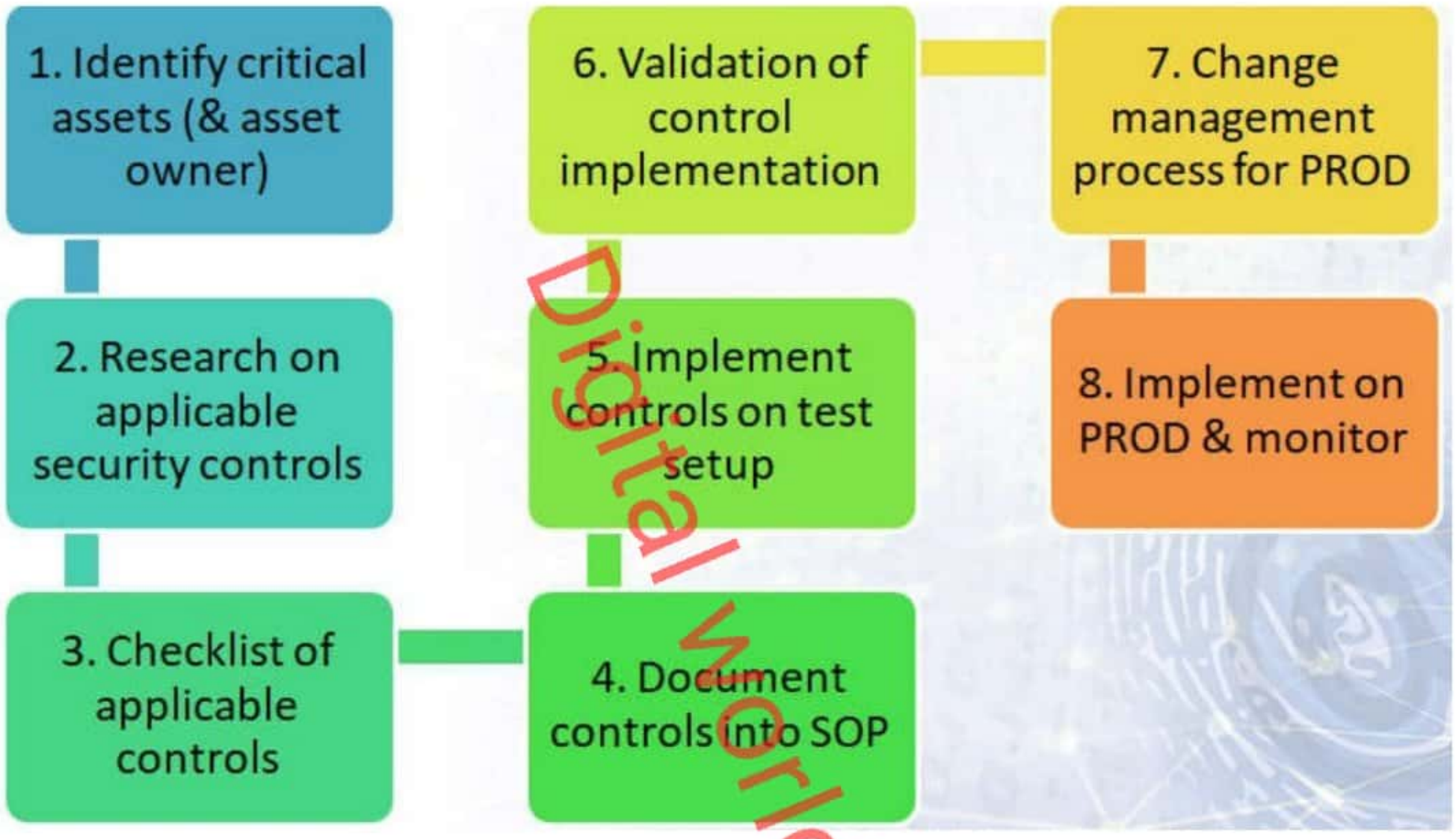
Question No 03: CIS and DISA compression?

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)

Question No04: Eight (8) step methodology ?

Ans:

8 STEP SECURITY HARDENING METHODOLOGY



Question 05: Pre-requisites For Security Hardening?

1. Security program approved
2. Consultant on board
3. Project kick-off meeting held
4. ISMC team identified and their loading for this project communicated
5. Appraisal linkage of core resources announced by CIO

Question No 06 : Consultant in Security Hardening?

1. Consultant on board
2. – Expert consultants in security transformation can facilitate the project success
3. – Third party & independent
4. – Bring a focus on delivering results
5. – Strong domain knowledge

Question No 07: Transformation model layers or Layers of security hadening transformation?

Ans:

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

Question no 08: Write any five steps in information security program?

1: Assessing security risks and gaps
2: Implementing security controls
3: Monitoring, measurement, & analysis
4: Management reviews and internal audit
5: Accreditation/testing

Question No 09: Who Are The Players In Information Security?

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

Question N0 11: SSh protocols versions names?

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

Question no 12 : 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

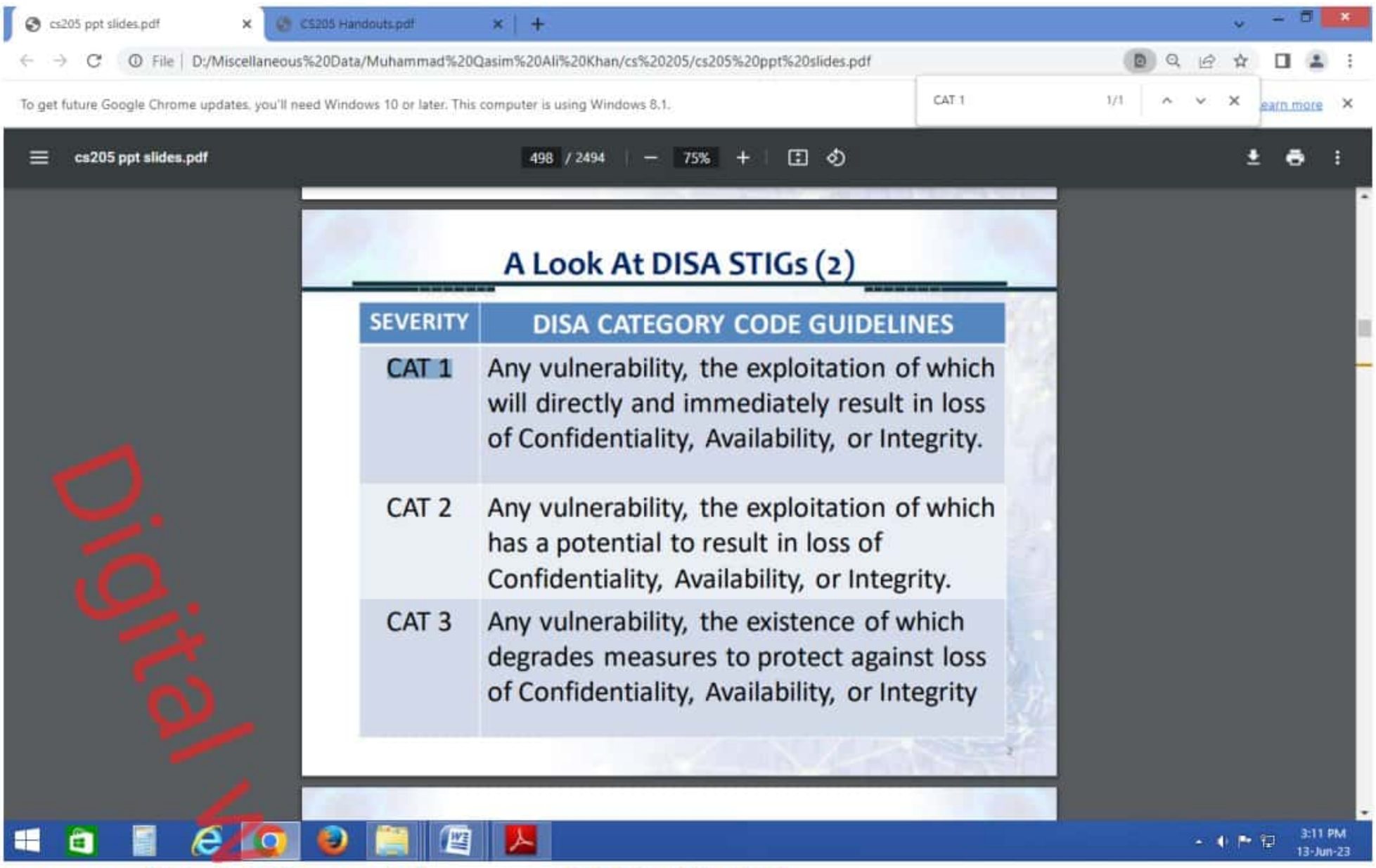
Question No 12 : Three pillars of information security Implemention: (yeh implementation hai)

- People
- Process
- Technology

Q No.13: 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**

Q no 14(Yeh table atta hai isko arrange kerna hota hai. Yuad ker lo isko. Most important)



Prepared By M.Qasim Ali 03337435091

Digital world Vu u tube channel (Follow and wtch)

Question No 15: Information security by SANS define

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

Question 16: 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)

Question no 17:Three types of redundant site models:

- Hot site
- Cold site
- Warm site

Question No 18: SIEM SOLUTION FOR SECURITY EVENTS DETECTION

Leading SIEM solutions:

LogRhythm,

IBM Q-Radar,

Splunk,

Elastic Search

Question No 19: Information Security Lifecycle steps

Requirements

2. Assess Current Posture

3. Remediation Plan

4. Implement Controls

5. Test/Validate

6. Accredit

7. Monitor & Audit

Question No 20: Yeh pic ho is k names likhne hote hain