CSA

* Risk Management :- Risk is the probability of a harmful event occuring as well as the potential to cause damage.
  ↓
  uncertainty that might lead to loss or damage

⇒ Threats :-

⇒ Vulnerability :- weakness / flaw / loophole
↓
(Physical, Admin, Soft, Hard, Comm., Personnel)

- Risk Analysis :- identifying most probable threats to an organization & analysing related vuln.
- Risk Assessment :- involves evaluating existing security & controls & assessing their adequacy relative to the potential threats of org.
- Risk Management :- Systematic application of mag. policies, procedures & practices to the tasks of establishing context, identifying, analysising, evaluating, treating, monitoring & comm. risks
  - Reactive (respond as they occur)
  - Proactive (reduces the risk of new vuln).

* Analytic Discipline
  - Risk Assessment
  - Management
  - Communication

* Examine
  - Availability
  - Eff
  - Costs
  - Implement & Monitor

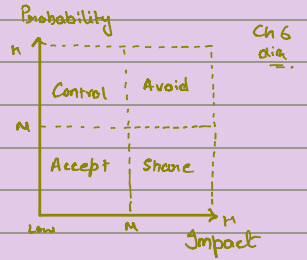
* Evaluate
  - Value
  - Vuln.
  - Threats
  - Risk

* Benefits of Risk Management
  - Assurance
  - Mechanism
  - Understanding
  - Support
  - Communication

⇒ Controls
↳ Safeguard or a measure to limit something

Process.

1. Resource Profiling - Describe resources & rate risk sensitivity.
2. Risk Assessment - Identify & rate.
3. Risk Evaluation
4. Document
5. Risk Mitigation
6. Validation - Testing
7. Monitoring & Auditing



Ch 6 dia.

6/11

Query → Observation (issue) → Report (NC) → non-compliant

Tool :- CSET - Used for assessment as per diff standard. - Free. Only for personal use. Not a commercial tool

Eg: CISA CPG, CISA RRA, NIST CSF, LMR Assessment,
↓
In USA
Acting like CERT-US.

CISA EDM,

- Maturity Model
- Diff Sectors
- NIST Special Pub.
- CIS Benchmarks.
- Financial
- SCADA

* egress - facing publicly outside
* ingress
* Strict source routing (already defined)
* Dynamic source "

Optical ring communication

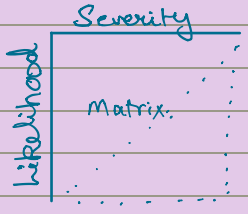
Risk Analysis

Que Diff b/w this.

Qualitative

- Positions
  Risk analyst
  Risk manager

→ Map all possible threats & probality of occurance.
→ Lengthy research • No need for historical data.
→ Also access controls
→ NOT Practical. (coz we dont get exact no).
→ Severity Score
  - Critical (Full access, prolonged outage)
  - High (Limited access, short disruption)
  - Medium (Indirect, degradation)
  - Low (no direct exposure)
→ Likelihood Scale
  - Negligible
  - Low
  - Moderate
  - High
  - Very high



Quantitative

This has to be done sooner or later.

→ Easy,
→ Looks for historical data
→ Requires time
- ALE :- Annual Loss Exposure.
- Risk = R. impact x R. Probability

Step 1: Identify Scope
Step 2: Assemble team
Step 3: Identify Threats
Step 4: Threat Prioritization
Step 5: Loss Impact
Step 6: Total Impact (Sum of threat priority & Impact priority).
Step 7: Identify controls / Safeguards
Step 8: Do cost benefits & coverage analy
Step 9: Rank Controls.
Step 10: Communicate Results

Risk registry ★ → Left.

18/11. BCP :- Business Continuity & Disaster Recovery Planning (BCP) (DRP).

* BIA :- Business Impact Analysis.
  ↳ determines proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecomm. services

* DRP :- (Contingency Planning) Disaster Recovery Plans
  ↳ Contains procedure for emergency response, extended backup operations & post-disaster recovery.
  ↳ Subset of BCP.

Que Diff b/w BCP & DRP
- BCP → Strategy, working etc., - Huge.
- DRP → One portion of BCP

* Business Disruption

Building Blocks

- Teams & Responsibility
- Cross-Trained Personnel
- Insurance
- Prioritisation of Activities
- Proper Doc.
- Effective Comm.
- Testing & Administration
- Periodic Review & Updation
- Emergency Procedures
- Recovery Strategy

* Why ?
1. Reduce Confusion
2. Resum normal business
3. Ensure survivability
4. Get running asap.

* Life - Cycle
* COOP.

[A] Sustain - Continous operation plan

[B] Recover / Resume Business Operations - Emergency or DRP.

[C] Protect business assets - Crisis Comm, Occupant (People, reputation, tangible assets). Emergency Plan (OEP).

Risk Registry.

↳ What docs are needed so that the logic & conclusions are clear ?
↳ Risk mitigation options.
↳ Evaluate the cost.

Risk	Risk level	Potential Cost/Benefit	External Controls to mitigate	Mitigation Techniques	Internal Controls (If needed).

Business Analysis tool. which is dynamic - AI - RBAC - BC.

20/11

☆ Process for Creating a BCP.

Loss
- Tangible → U can calculate → money, regulatory neg.
- Non-tangible → Can't calculate → Reputation

1] Project Initiation - project team & obtain mang. support, Business Continuity Coordinator
   a. Establish need
   b. Obtain mang. support
   c. Identify stakeholders & resources
   d. Create project mang. work plan.

2] BIA : (doc, identify fun' & criticality, prioritization, Analyse impact, Determine recovery windows & alternatives.
   ↳ management level fun. ↳ MTD - Max Tolerable downtime
   MTO - Max Tolerable outage.
   IRCTC downtime 11:30 to 12.
   a. Determine Info. Gathering Technique + Teams.
   b. Selected Interviewees.
   c. Identify Critical Business Functions.
   d. Analyze Information : & cost - qualitative & quantitative.
   e. Determine MTD & prioritization
   f. Threats
   g. Determine probability & risk
   h. Documentation & Communication

3] Recovery Strategy : Set of predefined & management approved actions implemented in response to a business interruption from a disaster.
   Natural / Man-made
   a. Document all costs assosciated with each contingencies
   b. Obtain cost estimates for any outside services (RFI, RFP, RFQ)
   c. Develop written agreements for outside services (SLA)
   d. Evaluate resumption.
   e. Identify BRP
   f.

Tier 2 - Infra: all over india
Tier 1 - Internet across globally.

Seismic zones
↳ divisions across tectonic plates
↳ earthquake.
Disaster recovery site
Should it be in one seismic Zone.

Elements / Types of Recovery

- Business
  - Critical
- Facility & Supply
- User
- Technical
  - Hot (24/7) · Expensive · Data not mirrored · Multiple Controls.
  - Warm · less cost · more eval. · No app · No data · Resources not dir. avail
  - Cold · critical infra · longer period · various loc. · Testing not poss. · Resources not quick immed.
- Data Recovery
  - mirror · Resources redundant · Info. distributed over multiple data center · No MTD · Expensive.
  - mobile · Self contained · Transportable · Full control · limited info processing capacity · Require advance coordination, · Resources not immediately available
  - Service Bureaus
  - Info, Telecomm, DCR.

Backup.
- Full - Complete file. 3 monthly, yearly.
- Incremental - Full file } around daily or weekly
- Diff - only changes

Coderonica → Synapse

4] Plan, Design & Development

a. Determine management concerns & prioritizes
b. Determine planning scope (geo concerns, org issues)
c. Establish Outage assumptions
d. Define prevention
e. Define resumption
6.
g. Develop Service fun. recovery plan

5] Implementation

6] Testing

- Structured walk-through :- Representatives come together as a group & walk through
- Checklist test :- 'OK' or 'NOT'.
- Simulation :- Virtual environment testing.
- Parallel Test :- Alternate site movement & then testing
- Full interruption test :- Entire 1° site is stopped & recovery site is tested.

7] Maintenance, Awareness & Training.

- Monitor

↓

Employees should be aware & trained as there is no specific post for that.

SCO
↓
Service level organization.

$(ISC)^2$: International Information Security cert Confers.

24/11

a

ISO: 27000 1 + 27000 2 — ISMS.

↓ Provides define (for certifications)

↓ Gives details of implementation (for procedural)

pager blast case study.

93 Controls

- → Org (37).
- → People (8)
- → Physical (14)
- → Technological (most followed as baseline - IT) (34)

(4 types of capacity : Storage, Network, Memory, Processing).

★ Scenario
→ Given a situation, make a list which covers everything with minimum controls

✱ People Control

1. Screening (Background, credit, academic screening)
2. T & Cs of employement
3. Info security awareness & training
4. Disciplinary process (fine, termination, committee manag.)
5. Respons after termination & Change of employement (employement termination, assets return back, data back)
6. Confidentiality or non-disclosure agreements
7. Remote working (WFH - VPN)
8. Information security event reporting

page burst

orig. equip manufac
OEM

✱ Organization

Guidance:
High - Information security policy
Low - topic specific policies

Considerations
- Business strategy & requirements
- regulations, legislation & contracts.
- Current & projected information security risks & threats

Low - Topic Specific
access control, info transfer, asset management.

1. Policies for Information security (defined, approved, published, communicated)
2. Information security roles & responsibilities.
3. Segregation of duties.
4. Management responsibilities.
5. Managing info security in ICT supply chain
6. Monitoring, review & change management of supplier services. (T&Cs of 3rd party (Supplier), some may accept, some not).
7. Info. Security for use of cloud services.
8. Info security incident manag. planning & preparation
9. Assessment & decision on information security events (If event will be considered as incident or accident or normal)
10. Response to info. security incidents. (responded to in accordance with the documented procedures).
11. Learning from information security incidents
12. Collection of Evidence. procedures for identification, collection, acquisition & preservation of evidence related to info security events. - effective management.
13. Information Security during disruption (maintainance during disruption)
14. ICT readiness for business continuity
15. Legal, statutory, regulatory & Contractual requirements
16. Intellectual Property rights
17. Protection of Records. (protect from loss, destruction, falsification, unauthorized access & release)
18. Privacy & Protection of PII.
19. Independent review of information security
20. Compliance with p
21. Documented Operating procedures (made doc available to personnel who need them - correct & secure operation of info processing facilities)
22. Contact with authorities (Escalation matrix - Roles)
23. Contact with special interest groups (Eg: CERT-IN., Subscription, Training)
24. Threat Intelligence (TTC - Tactics, Techniques & Procedure - Threat models - Threat intell collaboration (Virus Total, MISP)
25. Info. security in project management (collaboration or ppl involved in project - which info to share with whom).
26. Inventory of info. & other associated assets
27. Acceptable use of info. & other associated assets (what to use & how to use)
28. Return of assets (when transfer or resigned from org.) (in case of damage what to do)
29. Classification of info. (sensitive, public, secret, banking, PIIs)
30. Labelling of info. (Based on assets)
31. Information transfer (eg. private cloud. how data is shared among org).
32. Access Control
33. Identity Management
34. Authentication Information (passwd, OTP)
35. Access rights (Authorization, Admin, Guest etc)
36. Info security in supplier relationship
37. Addressing inf security in supplier agreements.

Making your own cloud

☆ Technical

1. User Endpoint devices (DLP, etc
2. Priviledge access rights (how to manage root/admin users)
3. Info access restriction (limitations like DBAdmin).
4. Access to source code (developers, only that project or module)
5. Secure Authentication (2FA, Multi-FA)
6. Capacity Management (Nagi OS - Storage - Processing - Memory - Network - will get alerts)
7. Protection against malware (Centrally mang. , Individually managed)
8. Management of technical vulnerability (Tools - when vuln is found, it will get an alert to you. - patch also (if available). ★ Minor Project.
9. Config management (Config Backup)
10. Information deletion
11. Data masking
12. Data leakage prevention (DLP - logging - FIM).
13. Information backup
14. Redundancy of info processing facility (Retention of Backup - SEBI - 8+ years).
15. Logging (all activities of all aged person).
16. Monitoring activities
17. Clock synchronization
18. Use of priviledge utility program (privilge access program - who should use)
19. Installation of software on operational security (procedure + restriction)
20. Network Security
21. Security of network services
22. Segregation of networks
23. Web filtering
24. Cryptography + Crypto Key Management.
25. Secure development life cycle
26. Application security requirement
27. Secure system architecture & engineering principles
28. Secure Coding
29. Secure testing in development & acceptance
30. Outsourced development (SLA should be there)
31. Seperation of development, test & product environments
32. Change management (version control) (tech, reviewer, approver)
33. Test information
34. Protection of info system during audit testing. (Not all info is shared).

★ Routing protocols
★ OSSec

Physical Controls

9/8/11

(old) FM200 - Gas Component - Prblm - human can't breadth naturally
Special mask is required.
It takes time (around 1 to 2 week) to
Supress the gas.

(new) Novec 1230 - can be easily compressed in an hour or 2.

Optimum temp = 18 to 22°C. (ideal).

Split AC + PAC (Precision (2nd generation) Air Conditioning) → ACs used in Data Center.
also CCU (Close Control Unit)

Next gen AC = Smart Racks.
= Expensive =
Each rack will have seperate cooling fans.

CRAC → disadvantage → insufficient CO2 above part didn't get proper cooling.
- 24/7
- Heater
- low/high humidity
- Access Remotely

Flooring would be up from the ground

- Environmental
- Generator Set
- Water leakage System
- UPS. - (Types, capacity, Backup time, 2 diff sources?).

★ HIPAA :- U.S.

↓ DHCS - Department of Healthcare Services

Congress parliament

1996

e-PHI - Protected Health Information → what it includes? - paper & comp files, x-rays, physician app. etc. Names, date, geo, No, Fax no, email, Social Security No, Medical record, Insurance plan, Acc No.

★ Rules

1. Privacy
2. Security Rule - Adm, Tech, Phy.
3. Breach Notification (72 hrs) from detection

8/12.

★ COBIT 5 :- (2012) Framework → Control Objective for Information & Related Technology.

latest ↳ 2019

↳ ISACA =>.

* 5 Key Principles

a. Meeting Stakeholder Needs - Create Value
b. Covering Enterprise End-to-End - Owners & Stakeholders → Governing Body → Management → Operations & Executions..
c. Applying Single integrated framework - Combines multiple standards together
d. Enabling Holistic Approach (7 points) - Principles, Org Stru, Processes, Culture, Ethics & Behaviour, Info, Services, Infrastr, People, Skills & competencies
e. Seperating Gov. from management.
   - Gov. → Evaluate, direct, monitor
   - Management → Build, Run, monitor

2019 Changes.

6 Key principles.

1. Stakeholders value
2. Holistic Approach
3. Dynamic Gov. System *
4. Gov. Distinct from Manag
5. Tailored to Enterprise needs *
6. End-to-End Governance System

Report

ATR - Action taking response

Obs - Risk - Recommen - Significance - Acceptance

CAAT — Tools: IDEA, ACL, Excel.

↳ Judgemental Sampling
↳ Statistical Sampling

Tools & Techniques which helps in auditing aka CAAT.

SOX — 2002. (July 30) - Goal of accounting & disclosure requirements.

↓

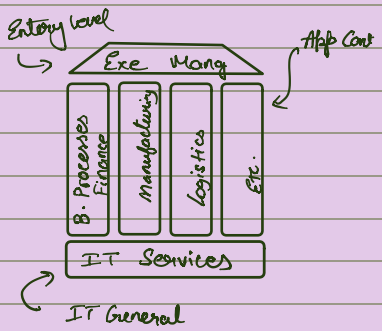
Sarbens

Oxely

Section 302 (fin. reporting)
Section 404 (accounting & financials).

Applicable :-

↳ publically held American companies
↳ accounting & 3rd party firms
↳ SEC.



PCI DSS

The 12 requirements of PCI DSS are:

1. Install and maintain a firewall configuration to protect cardholder data (review rules after every 6 months)
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data (Strong cryptography during transmission over public network. truncation or masking.)
4. Encrypt transmission of cardholder data across open, public networks (TLS, SSL)
5. Use and regularly update anti-virus software or programs (audit logs ON, so it can't be altered or removed by users)
6. Develop and maintain secure systems and applications (Security patches within a month - OWASP/SANS)
7. Restrict access to cardholder data by business need to know - PoLP, limited access to minimum data

TPA database

8. Assign a unique ID to each person with computer access (Authentication & Authorization)
9. Restrict physical access to cardholder data (POI devices?) (Retain visitor logs for minimum of 90 days).
10. Log and monitor all access to network resources and cardholder data (Automate logging & monitoring of user activity & retain logs for 1 yr. - Secure against unauthorized access & modification)

ISO PCIDSS IT

11. Regularly test security systems and processes (internal & external VA Scanning (CAVS) Quaterly • PT annually or after any significant change).

Intro Step Tech - CS Events Audit Disruptions Conclusions cp - Conferences Case Study IBM XFS tool

12. Maintain a policy that addresses information security for all personnel

13. Level 1 Merchants (Highest transaction volumes)
    - ↳ requires report on compliance (ROC)
      - ↳ by Qualified Security Assessor (QSA)

    Lower level typically uses self assessment questionnaire (SAQ)

14. De-Scoping
    - ↳ Network Segmentation or tokenization or P2P encryption reduces compliance efforts & risks

Unit 4.

Vulnerability — Threat — Risk — Controls
- Controls → proactive / reactive
- Implementation → Goal

Risk Analysis — identification — Qualitative & Quantitative
Risk Assessment — evaluating existing security & controls
Risk Management - systematic application - identifying, analysing, evaluating, treating, monitoring & communication

↓

Process
1. Resource profiling
2. Risk assessment
3. Risk Evaluation (Accept, Avoid, Mig, Transfer)
4. Document
5. Mitigate
6. Validate
7. Monitor

* Enterprise Risk Management Model.

1. Risk Identification - What could go wrong
2. Risk Analysis - Prioritization, check existing controls
3. Requirements identification - needed to prevent it?
4. Control Identification - list gaps
5. Risk Registry - Document

Risk	Risk level	Cost	External Control	Mitigation	Internal Control

---

* Need of BCP

1. Recover Quickly
2. Human life
3. Business Continuity
4. Operational & Financial loss ↓
5. Competitive Advantage
6. Immediate response to emergency
7. Internal & External threats
8. Major System & network failure
9. human or man-made disaster
10. minimise confusion & disorder

Eff. Comm
Periodic Reviews & Updation
Testing & Administration
Prioritization
Documentation
Teams & Responsibility
Cross-trained personnel.

* BIA :- Amt of impact an individual business unit can sustain to a significant interruption of of computing or telecommunication services.

BCP DRP diff

* DRP :- 1° obj is to provide capability to mission-essential applications in degraded mode & return to normal operational mode in reasonable amt of time.

* Business Disruption: Resources, personnel & business processes/tasks.

* Life Cycle of BCP

1. Sustain business operations
   - ↳ COOP (Continuity of operations Plan) HR
   - ↳ OEP (Occupant Emergency Plan) Firealarm
2. Recover or resume business operations
   - ↳ BCP
   - ↳ DRP
3. Protect business assets
   - ↳ Crisis Communication
   - ↳ Cyber incident response team

* Process of Creating a BCP

1. Project Initialization (needs) ∘ Establish need ∘ Obtain management support ∘ Identify stakeholders & resources ∘ Create project mgt workplan

2. BIA (define BCP requirements)

3. Recovery Plan — Types of Recovery, Types of Backup

4. Plan design & development
   - * Procedure for developing BCP.

5. Implementation
   - → BCP lifecycle

6. Testing ∘ Structured Walkthrough ∘ Checklist test

   Types → 1. Simulation (specific scenario env. simulated) 2. Parallel (Some sys. moved to alternate site & comp real process) 3. Full Interruption (Full shutdown of 1° site & recovery of business op. at alternate sites) → intrusive → Full blown drill → Risky → Approval needed

7. Maintainance, Awarness & Training
   - ↳ Monitor config management (CM) & update BCP plans accordingly
   - ↳ Plan & schedule BCP reviews
   - ↳ Distribute updates to BCP plans

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - ATKT Exam - Semester - I - July-2022

Subject Code: CTMSCS-SI-P2 **Date: 12-07-2022**

Subject Name: Cyber Security Audit and Compliance

Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Explain SOC Compliance in brief.	04
	(b)	State the difference(s) between policy and standard	04
	(c)	How to identify the proper security control for the protection?	08
		OR	
		Discuss HR Security control according to ISO27000 in detail.	
	(d)	Write a sample cyber security policy points and their requirements in industry.	09
Q.2	(a)	What are the good sign of an auditor.	04
	(b)	Discuss various types of audit in brief.	04
	(c)	Illustrate the importance of IT Act in a system.	08
	(d)	Explain Risk Management in detail.	09
		OR	
		Discuss Security rule of HIPAA in detail with all requirements.	
Q.3	(a)	Discuss various types of assessment methods.	04
		OR	
		What is Access Control? Discuss the various techniques to implement this control in computer system.	04
	(b)	What is logging and monitoring control.	08
	(c)	Write a note on COBIT-5.	09
	(d)	Discuss any realtime case study related to audit or assessment.	04
Q.4	(a)	What are the goals of audit.	
		OR	
		List all 7 domains of IT infrastructure.	04
	(b)	Explain Business Impact Analysis.	08
	(c)	Write a detailed note on Business Continue Planning.	09
	(d)	Explain the risk(s) in all seven domains of IT infrastructure respectively.	

*****

	(a)	Discuss Risk Assessment and Mitigation.
	(b)	Draw Structure of the standard of ISO 270001
	(c)	Explain about SOX - Sarbanes-Oxley Act and Compliance.

--- End of Paper---

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security

Semester – I – FINAL EXAM – REMEDIAL (June – 2024)

Subject Code: CTMSCS SI P2 **Date: 12/6/2024**

Subject Name: CYBER SECURITY AUDIT AND COMPLIANCE

Time: 2:00 PM to 5:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three.**	
	(a)	Discuss one Case study based on the importance of the audit.	08
	(b)	IT audit Approaches for Vendor and Third-Party Management.	08
	(c)	I. What is segregation of duties? II. How to maximize C-I-A of LAN domain.	08
	(d)	Explain Disaster Recovery & planning of DR	08
Q.2		**Attempt any three.**	
	(a)	Explain different Types of Audits with proper scenarios	08
	(b)	Define terms with Example or Scenario -Policies -Framework -Rules -Laws	08
	(c)	Explain Business Continuity Planning and life Cycle of BCP.	08
	(d)	What Are Controls and Why Are They Important?	08
Q.3		**Attempt any three.**	
	(a)	What Must Your Organization Do to Be in Compliance?	08
	(b)	Why Business Continuity Planning is required?	08
	(c)	What is the scope of an IT compliance audit?	08
	(d)	Discuss IT audit Approaches for Change Management.	08
Q.4		**Attempt any two.**	
	(a)	What is Risk analysis?	07
	(b)	Explain Remote Access in IT Domains for audit	07
	(c)	Write short note on Gramm-Leach-Bliley Act.	07
Q.5		**Attempt any two.**	

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security

Semester – I – January - 2024

Subject Code: CTMSCS SI P2 **Date: 12/01/2024**

Subject Name: Cyber Security Audit and Compliance

Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three.**	
	(a)	State the importance of Cyber Security Audit in the banking sector.	08
	(b)	In case of any disaster or manmade attack that disrupts organization's IT infrastructure and critical services. The organization want to continue their business in that situation. What is the solution? Explain that in detail.	08
	(c)	Discuss the Operations Security controls with respect to ISO 270001/2 standard.	08
	(d)	Explain remote access domain and discuss how to maximize C-I-A in this domain.	08
Q.2		**Attempt any three.**	
	(a)	Write a detailed note on Indian IT Act with their important sections.	08
	(b)	What strategies can be used to minimized the risk? Explain them in detail.	08
	(c)	How an organization can be in compliance? What they need to do?	08
	(d)	i) State the difference between Audit and Assessment. ii) State the difference between Qualitative and Quantitative risk analysis methods.	08
Q.3		**Attempt any three.**	
	(a)	Draw and discuss 7 domains of IT infrastructure in brief.	08
	(b)	What do you mean by control? Explain that and their various types in detail.	08
	(c)	Discuss various risk analysis strategies in detail.	08
	(d)	Explain LAN to WAN domain and also discuss various control.	08

1

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (December – 2024)

M.Sc. Cyber Security Semester – I

Subject Code: CTMSCS S1 P2 **Date: 05/12/2024**

Subject Name: Cyber Security Audit and Compliance

Time: 02:30 PM to 05:30 PM **Total Marks: 100**

Instructions:

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three.**	
	(a)	Why are governance and compliance important.	08
	(b)	Differentiate between Security Assessment and Security Audit.	08
	(c)	Define IT security audit and explain its objectives.	08
	(d)	Explain IT security Assessment, IT Security Audit and Security compliance.	08
Q.2		**Attempt any three.**	
	(a)	What is meant by scope of an audit? Explain its importance in the auditing process.	08
	(b)	How important is an IT Audit process.	08
	(c)	What is Computer Assisted Audit Techniques (CAATs), and why are they important.	08
	(d)	Write difference between Audit plan and Audit process.	08
Q.3		**Attempt any three.**	
	(a)	How to identify the risk level and how to write IT infrastructure audit report.	08
	(b)	What are the seven domains of a typical IT infrastructure? Briefly describe each.	08
	(c)	What are the key components of an IT infrastructure audit report?	08
	(d)	How to maximize CIA with the help of Audit and compliance.?	08
Q.4		**Attempt any two.**	
	(a)	What is risk analysis, and why is it important for organizations?	07
	(b)	What are the key phases of the BCP life cycle?	07
	(c)	How does disaster recovery planning differ from business continuity planning?	07
Q.5		**Attempt any two.**	
	(a)	Briefly describe the concept of Cyber Terrorism defined under the IT Act.	07
	(b)	Explain the purpose of ISO/IEC 27002 and its role in supporting ISO/IEC 27001.	07
	(c)	Discuss the significance of HIPAA in protecting healthcare information.	07

--- End of Paper---

1

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - I - Jan-2023

Subject Code: CTMSCS SI P2 **Date: 09/01/2023**

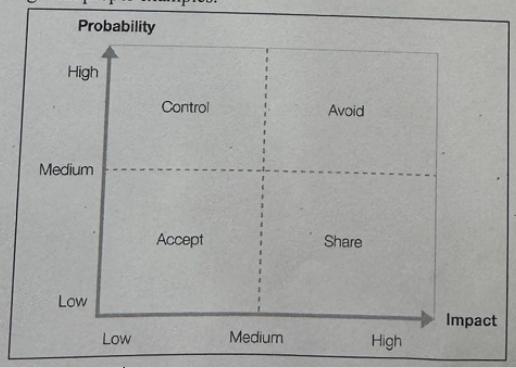
Subject Name: Cyber Security Audit and Compliance

Time: 11:00 – 14:00 **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	What is Access Control? Explain the effective solutions to implement this control.	04
	(b)	Define the following term. • Risk Analysis • Governance • Compliances • Risk Mitigation	04
	(c)	Explain the Operations Security control according to ISO 27000 standard in detail.	08
	(d)	Write a detailed note on COBIT5.	09
Q.2	(a)	Explain SOC Compliance Reports briefly.	04
	(b)	State the difference between Guideline and Policy.	04
		OR	
	(b)	How to maximize C-I-A of workstation domain.	04
	(c)	Read the figure given below and explain all risk management strategies along with proper examples.	08



	(d)	Explain any 5 controls of IT Infrastructure with its risk, recommendation and example.	09
Q.3	(a)	Write full form of the following: i) HIPAA ii) NIST iii) PCI-DSS iv) BCP	04
	(b)	What are the classification of Information?	04
	(c)	Discuss Disaster Recovery Planning and its various strategies.	08
		OR	
	(c)	What Must Your Organization Do to Be in Compliance?	08
	(d)	Describe the life cycle of BCP.	09
Q.4	(a)	What is segregation of duties?	04
		OR	
	(a)	How to maximize C-I-A of LAN domain.	04
	(b)	Explain CAAT with various application control.	04
	(c)	If you are an auditor, then explain the process of cyber security audit carried out by you.	08
	(d)	Discuss the process of selecting and implementing effective controls in an organization.	09
		OR	
	(d)	Write a note on GDPR and its articles.	09

*****

END OF PAPER

NATIONAL FORENSIC SCIENCES UNIVERSITY

MSc Cyber Security - Semester - I – ATKT SEE - June -2023

Subject Code: CTMSCS SI P2 **Date: 27/06/2023**

Subject Name: Cyber Security Audit and Compliance

Time: 11:00 AM to 02:00 PM **Total Marks: 100**

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	What is Risk in IT environment?	04
		OR	
	(a)	What is compliance?	04
	(b)	Brief about the Cyber Security Audit.	04
	(c)	Write a detailed note on 'controls' with its types and selection process.	08
	(d)	Illustrate the cyber security audit importance in the industry in your words.	09
Q.2	(a)	What is the scope of the audit?	04
	(b)	Discuss the difference between policy and standard.	04
	(c)	Explain the importance and requirement of security policy and procedure in an organization.	08
		OR	
	(c)	Explain any real-world case study related to cyber security audit and compliance.	08
	(d)	Discuss the maximization of C-I-A in Workstation and LAN domain.	09
Q.3	(a)	Discuss the Business Impact Analysis.	04
	(b)	Give brief description about SOC compliance.	04
	(c)	Write a detailed note on Business Continuity Planning.	08
	(d)	Write down operations security controls with respect to ISO 27001.	09
		OR	
	(d)	Explain the process of achieving compliance in an organization.	09
Q.4	(a)	What is the Risk Assessment?	04
		OR	
	(a)	Write list of 7 domains of IT infrastructure.	04
	(b)	Draw 5 principles of COBIT5.	04
	(c)	Write the detailed note on HIPAA.	08
	(d)	Give details of IT Act section 66 and its subsections	09

Q.4		**Attempt any two.**	
	(a)	What do you understand by CAAT? Explain it's importance in audit with an example.	07
	(b)	Explain various disaster recovery strategies.	07
	(c)	Discuss base line security controls and its importance.	07
Q.5		**Attempt any two.**	
	(a)	You are IT manager in your organization and joined recently. Due to last audit non compliance you have been given charge to select and design proper security controls for your organization. What and How will you complete the task with respect to any applicable law and standard? Explain the process.	07
	(b)	Write a detailed note on HIPAA with its rules and safeguards.	07
	(c)	How to maximize C-I-A of user and LAN domain.	07

--- End of Paper---

Hippa – 1996

↳ Portability - Ability to transfer & continue health insurance of workers even if their job changes
↳ Fraud Reduction
↳ Standardization - ebilling & healthcare info. processes.
↳ Protection (PHI)

*Rules
→ Not to disclose or discuss about patient details in public or if not related

- 3 main Rules
  ↳ Privacy Rule – when & how PHI can be disclosed - paper, e, oral
  ↳ Security Rule – ePHI – implementing controls/safeguards to ensure CIA.
  ↳ Breach Notification – Notify about breach to individuals, US dep of health & human Serv & media

⇒ 2011 Pilot Audit – Completed in 2012 – Breach of all 3 Rules.

- PHI – Protected Health Information
  ↳ considered in any form electronic, paper, xray, appointment
  ↳ 18 identifiers
    a. Demographics – Name, No, email, location
    b. Medical / legal – Medical record no, Acc. No, Health plan beneficiary nos.
    c. Technical :- IP, URLs, device ID/serial no, Vehicle ID.
    d. Biometrics :- Fingerprint, retina, full-face
    e. Dates :- (other than yr) related to individual
    f. Others :- unique id, char, code

Diff b/w PHI & ePHI.

- Controls

Policies, Sanctions & Training Should be there.

Technical	Administrative	Physical
• Access Control	• Risk Analysis + Mang	• Workstation Security
• Audit	• Security Personnel	• Facility Access Control
• Integrity	• Workforce Training	• Device & Media Controls
• Transmission security	• IR Procedure	• Physical Protection of Servers
• Unique ID	• BAA	• Media Movement
• Auto logoff	• Sanctions	
	• Emp. oversight, pass. mang	
	• Login • Response & Reporting	
	• Contingency Planning	
	• Evaluations	

Terms
Required
Addressable

⇒ Complain can be filled with office for Civil Rights (OCR)
Covered entities & bussiness associates would be under investigation.

⇒ Penalties & Alarm :- BAA → Covered Entities → Individuals (written or mail / phone) → within 60 days period
↳ Should have description - steps - action
↳ on website or media info should be there for 90 days
↳ Civil – 100 to 50,000 $s
↳ Criminal – 250,000 $s.

→ Sharing info from 1 physician to another in secure way is allowed
⇒ Contingency & Disaster Recovery Plan
↳ BCP ↳ DRP ↳ Sites ↳ Test
⇒ Risk Analysis & Risk management

- HIPAA Requirements for website
  1. Transport Encryption
  2. Storage Encryption
  3. Backup
  4. Sharing
  5. Authorization
  6. Integrity
  7. Disposal – permanently erased

- Why HIPPA?
  → more control to patients
  → Set boundaries on use & disclosure
  → Accountability
  → Responsible disclosure

★ Employement Record

★ Court Order & Subpoena
(issued by judge) + should share info but only specific
(issued by other than judge eg court clerk) ↳ provider must receive evid. / proof that individual was notified to object

★ Research ★ Public health concerns

COBIT :- Control Objectives of Info & related technologies.

→ It is a framework given by ISACA for IT management & IT governance.
→ It provides implementable set of controls over IT & organizes them around a logical framework of IT related enablers

COBIT	1	2	3	4	5
	1996	1998	2000	2005/7	2012
	Audit	Control	Mang.	IT Gov	Gov. of enterprise IT

★ 5 Key Principles

1] Meeting Stakeholder Needs – Creating value for stakeholders → Transforming needs to actionable, specific & customizable goals

2] Covering Enterprise End-to-End – Owners & Stakeholders → Governing Body → Management → Operations & Executions.. [Covering entire enterprise fun² & process – IT as asset]

3] Single Integrated Framework – It aligns with other major standards like ISO/IEC 9000, 38500 or TOGAF
Unifying governance structure

4] Enabling Holistic Approach – 7 enablers :- • People, Skills & Competencies • Service, Infra & App.
• Process • Information • Org Structure
• Principles & Policies • Culture, Ethics & Behaviours

5] Seperating Governance from management –
(Board level) E (Evaluate) D (Direct) M (Monitor)
(Executive level) P (Plans) B (Builds) R (Runs) M (Monitors)

★ Drivers
↳ Keeping risk at acceptable level
↳ Comply to laws
↳ Maintaing availability to systems

• Enterprise Benefits
• Stakeholder Values
★ 8 Benefits
• Complexity reduced • improved integration • Better Cost management • Informed risk decisions.

In 2010 ISACA, ISC², ISF worked together to create 12 principles
• Support buss. • Defend buss. • Promote responsible Inf. sec. behaviours

★ Implementation life cycle (Continous, not 1 time)
1. Program Manager (outer)
2. Change Enabler (middle)
3. Continual improvement life cycle (inner)

→ COBIT for security professionals. It guides how to establish & manage business policies & processes ensuring CIA is maintained for information (Should have scope, validity & Goals)

✱ Life Cycle of BCP

1. Sustain Business Operations
   - → COOP (Continuity of Operation Plan)
     Key business fun' continue without major interruption

2. Recover / Resume Business Operations
   - BRP (Non tech) operations to resume after disruption
   - DRP (Tech) IT Recovery
   - IT Contingency (How it will work) during outages
   - Cyber Incident Response Plan

3. Protect Business Assets
   - OEP (Occupant Emergency Plan)
     - Ppl safety - assembly point, emergency comm., evacuation
   - → Crisis Communication
     [People, Reputation, Tangible assets]

✱ Steps of BCP making :-

1. Project Initialization - Stakeholder, Team, T.L., need for BCP.
2. BIA - MTD
3. Recovery - Types, Backup types, levels, Recovery sites, offsite storage
4. Plan, design & develop - Cost, approve, analyse
5. Implementation - COOP, IT Contingency, DRP, OEP
6. Testing - Walkthrough Structured - Types 11, simulation, full interruption
7. Maintainance - Awarness, Training