# Exam Preparation session
## (MCQ Modules 2,3,4,5: DISSA Course)

**Arijit Chakraborty**

***August 01 , 2021***

# Module 2- Compliance and Security Framework

- SOX
- PCI DSS
- NIST
- SSAE 16
- AT 101
- FEDRAMP
- HIPAA / HITECH
- ISO 27001
- GDPR
- PDP Bill
- IT Act 2000, Amendment 2008, Rules 2021

## Module 2 - Compliance and Security Framework

- 1. PCI DSS stands for _____
- A. Petro Carbon Industry Decision Support system
- B. Professional Computing Institute – Digital Standard System
- C . Processing Card industry – Dedicated Security Service
- D. Payment Card Industry – Data Security Standard
- Answer - d

- 2. As per PCI DSS, “System components” include which of the following :
- A. network devices,
- B. servers,
- C. computing devices
- D. applications.
- **Options**
- 1. A&B only
- 2. B&C only
- 3. A,C,D
- 4. A,B,C, D
- Answer = 4

- 3.The PCI DSS has ___ important principles / requirements
- A. 10
- B. 12
- C. 14
- D. 20
- Answer = B

- 4. The PCI DSS advocates
- A. using vendor supplied passwords for users
- B. keeping default passwords unchanged
- C. documenting the factory-default settings
- D. not to use vendor-supplied defaults for system passwords and other security parameters
- Answer - d

- 5.In the context of IS Security , ‘SIEM ‘ indicates :
- A. Software Implementation & Exposure Management
- B. System Inclusion & Enterprise Monitoring
- C.  Software Induced Energised Management
- D. Security Information and Event Monitoring
- Option = D
- (SIEM), can help to  log system and network activities, monitor logs and alert of suspicious activity

- 6. The NIST Framework has been developed by ____ and originates from ____ country :
- A. National Institute of Standards and Technology , USA
- B. National Institute of Science & Technology , France
- C. National Institution of Software Technology , UK
- D. National Institute of Systems and Technology, Germany
- Answer – a
- **National Institute of Standards and Technology** -federal agency within Department of Commerce that spans manufacturing, quality control, and security,
- Collaborates with security industry experts, other government agencies, to establish **set of controls & balances** to help operators of critical infrastructure manage cybersecurity risk

- 7.  NIST Cyber Security framework excludes which of the action points ?
- A. Identify
- B. protect
- C. detect & respond
- D. escalate & terminate
- Answer - d

- 8. SOC -2 & 3 deals with :
- A. internal control on financial reporting for service organisation
- B. Standards for IS audit of subsidiaries
- C. IS Audit system for listed companies
- D. operational, process, software, procedure, data controls for service organisations
- Answer = d

- 9. FedRAMP deals with
- A. IT Controls in private companies
- B. standardized way for government agencies to evaluate the risks of cloudbased solutions.
- C. Blockchain technology in banking sector
- D. AI use in Government sector projects
- Answer = b

- 10. HIPAA stands for
- A. Highly Intelligent Performance Accountability Act
- B. Health Integrated Protection Accounting Act
- C. Holistic Insurance Protection Assurance Act
- D. Health Insurance Portability and Accountability Act
- Answer - d

- 11. HIPAA is applicable usually for _____ sector and encompasses _____
- A. Healthcare , privacy rule & data encryption
- B. healthcare , public access and usage of data
- C. banking & Insurance , breach concealment
- D. Health & fitness , sharing of Private sensitive data in public platform
- Answer – a

- 12. ‘Cookies ‘ in IS Security domain, means
- A. Open-source  software used for games & entertainment
- B. advanced apps used for learning cooking different recipes
- C. Small data file that is placed on computer or other device to allow a site to recognize visitor as a user when he returns to the Site using same computer and web browser
- D. advanced type of biometric security
- Answer – c

- 13. Relevant Auditing Standards used for Risk assessment of client organisation is :

A. ISA 300

B. ISA 315

C. ISA 320

D. ISA 405

Answer - B

- 14. IDEA audit software is used for a
- A. display, analyze, manipulate data
- B. sample or extract from data files
- C. data importing, extraction and analysis.
- D. all of the above
- Answer – d

- 15.As per the Personal Data Protection Bill,India, **Sensitive Personal data & Info** ( SPDI) includes :
- A. Biometric data,
- B. Caste or tribe,
- C. Religious political belief or affiliation
- D. Passwords
- **Options**
- 1. only A and D
- 2. B& C
- 3. A , B, D
- 4. All four
- Answer - 4

- 16.Section 40 of the PDP Bill, India ,deals with:
- A. Personal and Sensitive Personal Data of Children
- B. Data Principal Rights
- C. Penalties, Remedies and Offences:
- D. Transfer of Personal Data Outside India:
- Answer – d

- 17. ISO 27001 is the governing standard for
- A. Acquisition of Hardware & software
- B.  Ensuring software piracy
- C. ensuring software and hardware privacy
- D. information security management system (ISMS).
- Answer – d

- 18. _____ is the practice and precautions taken to protect valuable information from unauthorised access, recording,
- disclosure or destruction.
- (a) Network Security
- (b) Database Security
- (c) Information Security
- (d) Physical Security
- Answer - c

- 19. Compromising confidential information comes under _____.
- (a) Bug
- (b) Threat
- (c) Vulnerability
- (d) Attack
- Answer = b
- **Explanation: Threats are anything that may cause damage or harm to a computer system, individual or any information.**
- Compromising of confidential information means extracting out sensitive data from a system by illegal manner

- 20. Lack of access control policy is a _____
- (a) Bug
- (b) hacker's Threat
- **(c) Vulnerability**
- (d) external Attack
- Answer- c
- **Explanation: Access control policies are incorporated to a security system for restricting of unauthorised access to**
- any logical or physical system. Every security compliance program must need this as a fundamental component. Those
- systems which lack this feature is vulnerable.

# Module 3: BCP & DRP

- BCP –DRP Overview
- Key terms & concepts
- RPO, RTO
- Pre DR ICQ, BCDR Process Flow
- BC DR QRH
- BCP- Internal Audit Role – IIA Guidelines
- DRaaS : BC DR Software capabilities
- BCDR – Detailed IS Audit Checklist
- ISO 22301 – BCM

- 1. In planning for DRP, ‘disaster ‘ can be :
- A. Geological:
- B. Meteorological & Health
- C. Man-made
- D. all the above
- Answer – d

- 2. Which is the most vital objective of BCP & DRP Systems ?
- A. confidentiality of data
- B. integrity of data
- C. availability of data
- D. audit of data
- 3. To audit BCP, IS Auditors must review the _____ document of the client , as the primary source
- A. IT Policy
- B. Segregation of duties
- C. Business Impact Analysis ( BIA)
- D. SLA with vendors
- Answer – c

- 4. Which ISO Deals with Business Continuity Management Systems ( BCM)
- A. ISO 27001
- B. ISO 31000
- C. ISO 22301
- D. None of the above
- Answer- c

- 5. Period of time from disaster onset to resumption of business process , based on acceptable downtime, is referred to as :
- A. Disaster Duration Time ( DDT)
- B. Breakdown Time analysis ( BTA)
- C. Recovery Time Objective ( RTO)
- D. Machine Down time ( MDT)
- Answer – c
- 6. Achievement of Near-zero RPO implies :
- A. Less expense and infrequent data back-up
- B. moderate expense and weekly data back –up
- C. An impossible situation which cannot be achieved in practice
- D. very expensive and ensuring continuous data replication
- Answer - D

- 7. ___ back-up sites are fully configured & ready to operate within several hours and are usually intended for emergency operations of a limited time period
- A. Frigid
- B. cold
- C. warm
- D. Hot
- Answer – d
- 8. _____ site offers no hardware equipment, telecom and the set up time is normally _____
- A. hot, low
- B. warm, low
- C. cold , high
- D. depends on SLA
- Answer - c

- 9. Most enterprises create BCP for ____ processes
- A. business critical
- B. mission critical
- C. vision critical
- D.  All
- Answer = b
- 10. Detailed data, lowest level data can be backed up and recovered using _____ technology
- A. Nano
- B. Micro-recovery
- C. Base recovery
- D. Granular Recovery
- Answer = d

# Module 4 : Cyber Security, Threat & Forensics

- Common Cyber Attacks
- Phishing / Social Engineering Attacks,
- DoS, DDoS, Ransomware, Internal Attacks
- Vulnerability and Threat Analysis
- Digital Forensics- Audit steps
  Common Cyber Attacks
- Deception Technology – Honeypot
- Cryptography and Steganography,
- Digital Evidence
- Ethical Hacking
- Network Communication, hardware components
- Firewall Protection, Virtual Private Networks
- Antivirus and Antimalware Software
- Transmission Control Protocol (TCP/ IP)
- Demilitarized Zones (DMZ)

- 1. Malicious pursuit for making network resource or server unavailable for users, by disrupting or suspending services of hosted connection of Internet is termed _____
- A. hacking
- B. cracking
- C. keylogging
- D. Denial of Service attack (DoS)

- 2. In a _____ attack, the hacker tries various combination of passwords, usernames, again & again until entry obtained
- A. Biting
- B. Bot-net
- C. Brute Force
- D. Crude –open
- 3. Phishing and Spoofing are examples of :
- A. internal controls
- B. IS Audit tools
- C. malicious attacks on IT system
- D. software patches

- 3. Computer Security Experts and specialists in penetration testing and professionals who constantly defend growing technology to fight criminally-minded hackers are referred to as :
- A. White cat hackers
- B. Black Belt hackers
- C. Black Cat hackers
- D. white hat hackers
- Answer = d

- 4. Ransomware is a type of :
- A. Advanced software for data analytics
- B. IS Audit tool used in high-end ERP environments
- C. crypto currency software used globally
- D. malicious attack on IT Systems and data and then to demand money from victim

- 5. _____ is a network-attached system set up as  decoy to lure cyber attackers & detect, deflect , study hacking attempts
- A. money-pot
- B. honeypot
- C. sweetmeat
- D.  Router
- Answer = b
- 6. IT Security system that requires 2 separate, distinct forms of identification in order to access is called
- A. Double-doze system
- B. Dual Lock System
- C. Twin Factor testing
- D. 2FA
- Answer = d

- 7. If DELHI is coded as CCIDD in a cryptography system , how to encode BOMBAY?
- A.  AMHDFO
- B. AZSWEU
- C.  AWESOM
- D. AMJXVS
- Algorithm :  (order :  -1, -2,-3, -4, -5)
- Answer - d

- 8. _____ implies a technique of hiding secret data within ordinary, non-secret, file or message in order to avoid detection.
- A. Typography
- B. cryptography
- C. telegraphy
- D. Steganography
- Answer – D
- 9.Which one is not a  Network topology ?
- A.  Star
- B. mesh
- C. bus
- D. car
- Answer – d

- 10. _____specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination
- A. VOIP
- B. TCP/IP
- C. Media over Internet
- D. EDI
- Answer – b

- 11. ___ transmit signals in form of light between two ends of fiber hence they permit transmission over longer distances & at higher bandwidth than coaxial & twisted pair cables or electrical cables.
- A. Electrical cable
- B.co-axial cable
- C. twisted pair cable
- D. fiber optic cable

- 12. Internal Audit in IT Environment is governed by _____ issued by the Institute of Chartered Accountants of India
- A. SIA 11
- B. SIA 12
- C. SIA 13
- D. SIA 14
- Answer - d

# Module 5- Business Application – Acquisition, Development & Implementation

- Audit Charter, IS Policy
- IS Audit process details
- ToR / EL & NDA
- IS Audit Approach
- Application of SIA
- IS Audit Reporting
- Data analytics
- HW & SW Acquisition
- Blockchain
- RPA
- AI
- Cryptocurrency
- IoT

- 1. ____ is the apex regulatory body regarding cyber – related matters and IT in India
- A. SFIO
- B. CBI
- C. CERT-In
- D. ED
- Answer –c

- 2. Scope limitations , if any, and restriction on distribution and usage of IS Audit report should be mentioned in :
- A. Internal Audit charter
- B. IT Policy
- c. IS Audit Report
- D. all of the above
- Answer – c

- 3. IT Vendor support should be sought in :
- A. hardware
- B. software
- C. installation & testing
- D all the above
- Answer= d
- 4. ____ technology enables  a system of interrelated computing devices, mechanical & digital machines, objects, animals or people provided with unique identifiers (UIDs) & ability to transfer data over network without human-to-human or human-to-computer interaction.
- A. Intranet of things
- B. Internet of things
- C. VOIP
- D. TCP
- Answer- b

- 5.RPA Ecosystem consists of :
- A. process developers & users
- B. business users
- C. Robot controllers
- D. all the above
- Answer – d

- 6. Cognitive Automation has which of the following capabilities
- A. Natural Language Generation & understanding
- B. processes structured data only
- C. basic Pattern recognition
- D. none of the above
- Answer = a

- 7. Which of the following is true ?
- A. ML is a subset of DL
- B. AI is a subset of DL
- C. ML is the super-set of AI
- D. ML is a subset of AI
- Answer = d

- 8. In conducting IS Audit of RPA and AI Systems, a very critical area to review is :
- A. check IT policy
- B. examine SOD for RPA use
- C. evaluate enterprise technolgy expertise
- D. review how instructions scheduled in RPA tool, and perform testing of edit, validation check, error check, etc., configured in RPA
- Answer – d
- 9. Which one of the following is NOT a known AI type ?
- A. Prescriptive
- B. Descriptive
- C. predictive
- D. prognostic
- Answer- b

- 10.Blockchain depends on which technology ?
- A. CLT
- B. Cryptography
- C. Steganography
- D. DLT
- Answer – d
- 11. Automated contracts , embedded in block chain in the nature of self-executing contracts with terms of agreement between buyer & seller directly written into lines of code is called _____
- A. Block contract
- B. Chain contract
- C. Digital contract
- D.. Smart contract
- Answer - d

- 12. Only authorised & known participants can write and commit in a _____ blockchain
- A. permissioned –public
- B. private – permissioned
- C. public – permissionless
- D. private – permissionless
- Answer – a
- 13. Cryptocurrency (PVC) are issued by _____
- A. central bank
- B. Sovereign / government
- C. commercial banks
- D. private players
- Answer – d
- 14. RBI is planning a phased launch of :
- A. Private Crypto-currency
- B. new currency notes
- C. E-currency
- D. CBDC
- Answer - d