Fast Track Webinar Series

VISA *for* DISA

Day 2

ICAI Information Systems Audit 3.0 Course

15th Batch

INFORMATION SYSTEMS AUDIT 3.0 COURSE

Module - 5

Protection of Information Assets

Tuesday ◊ 27th JUN 2023 ◊ 08:30 PM to 09:30 PM ◊ www.3spro.blogspot.com

CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional, Registered Valuer & Arbitrator

Visiting Faculty, Indian Institute of Management

Pointers

- ISA 3.0 (new syllabus) is an enriched version of ISA 2.0 (old syllabus). Not to be distinguished
- Read the ICAI Study Material minimum 2 - 3 times for getting clarity and confidence
- **Exam Preparation Tip: Practice eliminating the three choices by reasoning**
- All references made in this material is based on the following BGM of ICAI – Module 5 – Protection of Information Assets

https://resource.cdn.icai.org/60975daab49637bgmisa-mod5.pdf

Reference Material for ICAI ISA PQC

Basic

- ISA Background Material 3.0
- DISA AT Mock Test Papers

Additional

- Security in Computing, 3rd Edition, By Charles P. Pfleeger, Shari Lawrence Pfleeger Published Dec 2, 2002 by Prentice Hall.
- ISA 2.0 Background Study Material
- http://compnetworking.about.com/
- http://theirm.org/
- http://www.cert.org/
- http://www.isaca.org/
- http://www.iso.org/iso/home/standards/iso31000.htm

Reference Material for ICAI ISA PQC

Additional

- http://www.webopedia.com
- https://na.theiia.org/Pages/IIAHome.aspx
- https://www.dataprotection.ie/
- www.ehow.com
- www.en.wikipedia.org
- www.firesafetyinstitute.org
- www.resources.infosecinstitute.com/access-control-models-and-methods
- www.technet.microsoft.com/en-us
- https://owasp.org/www-project-top-ten/
- https://en.wikipedia.org/wiki/Threat_model#Threat_modeling_tools
- https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)
- https://en.wikipedia.org/wiki/STRIDE_(security)
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf
- https://en.wikipedia.org/wiki/Separation_of_duties

ISA 2.0 and ISA 3.0 comparison (with weightage)

Weightage	ISA 2.0	ISA 3.0
18%	Primer on Information Technology, IS Infrastructure and Emerging Technology	Information Systems Process Audit
12%	Information Systems Assurance Services	Governance and Management of Enterprise Information Technology, Risk Management, Compliance and Business Continuity Management
12%	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	System Development, Acquisition, Implementation and Maintenance Application System Audit
18%	Protection of Information Systems Infrastructure and Information Assets	Information Systems Operations and Management
12%	Systems Development: Acquisition, Maintenance and Implementation	Protection of Information Assets
6%	Business Continuity Management	Emerging Technologies
12%	Business Applications Software audit	
10%	Project Report	

Module 5
Protection of Information Assets

✓ Introduction to Protection of Information Assets	5.1
✓ Administrative Controls of Information Assets	5.2
✓ Physical and Environmental Controls	5.3
✓ Logical Access Controls	5.4
✓ Network Security Controls	5.5

Chapter 1

Introduction to Protection of Information Assets

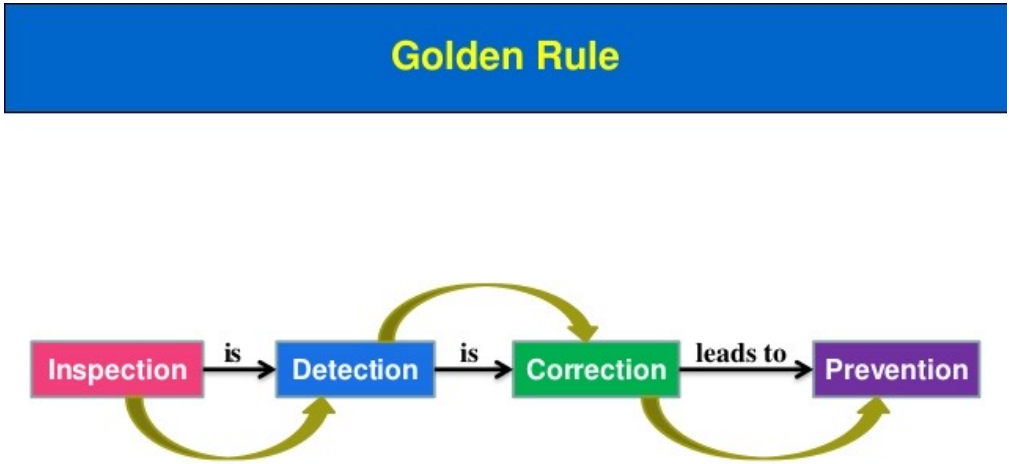
1. Which of the following shall BEST help in deciding upon the protection level for information asset?

a) Location of asset.

b) Impact of risk.

c) Vulnerabilities in asset.

d) Inventory of threats



2. Which of the following is a risk response option?

a) Determine likelihood of threat

b) Determine probability of risk

c) Deciding amount of insurance cover

d) Prepare risk profile report

Negative Risk

There are four possible risk response strategies for negative risks:

- **Avoid** – eliminate the threat to protect the project from the impact of the risk. An example of this is cancelling the project.
- **Transfer** – shifts the impact of the threat to as third party, together with ownership of the response. An example of this is **insurance.**
- **Mitigate** – act to reduce the probability of occurrence or the impact of the risk. An example of this is choosing a different supplier.
- **Accept** – acknowledge the risk, but do not take any action unless the risk occurs. An example of this is documenting the risk and putting aside funds in case the risk occurs.

Positive Risk

There are also four possible risk responses strategies for positive risks, or opportunities:

- **Exploit** – eliminate the uncertainty associated with the risk to ensure it occurs. An example of this is assigning the best workers to a project to reduce time to complete.
- **Enhance** – increases the probability or the positive impacts of an opportunity. An example of this adding more resources to finish early.
- **Share** – allocating some or all of the ownership of the opportunity to a third party. An example of this is teams.
- **Acceptance** – being willing to take advantage of the opportunity if it arises but not actively pursuing it. An example of this is documenting the opportunity and calculating benefit if the opportunity occurs.

3. After a Tsunami, a business decides to shift the location of data centre from coastal area to mid land. Which type of risk response option it has exercised?

a) **Accept**

b) **Avoid**

c) **Mitigate**

d) **Transfer**

4. Organizations capacity to sustain loss due to uncertainty and expressed in monetary terms is best known as:

a) Risk appetite

b) Risk tolerance

c) Risk acceptance

d) Risk mitigation

5. Main use of maintaining and updating risk register is to:

a) Define controls

b) Identify risk owner

c) Built risk profile

d) Maintain evidence

A **risk profile** is an evaluation of an individual's willingness and ability to take **risks**. It can also refer to **the** threats to which an organization is exposed. Example: Health Risk Profile

6. Of the following, who is accountable for deciding and implementing controls based on risk mitigation plan?

a) Chief Risk Officer

b) Risk owner

c) IT operations manager

d) Board of directors

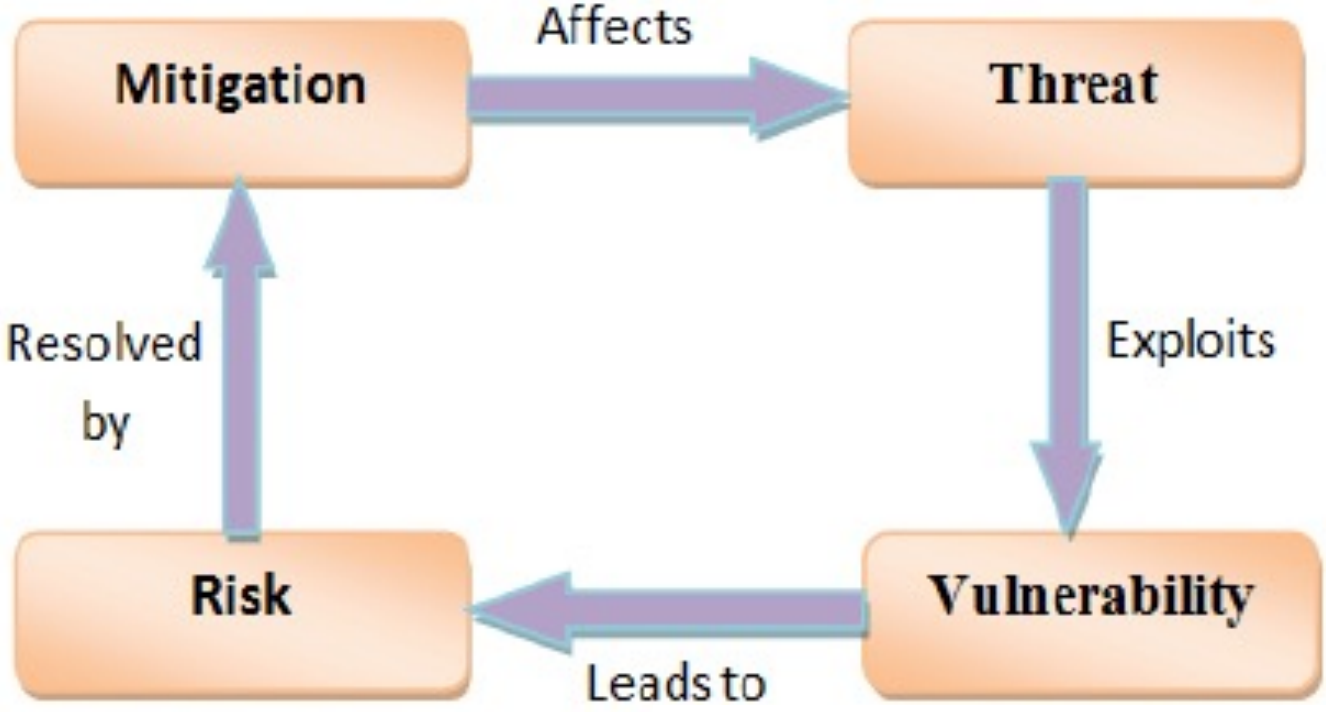
7. Which of the following is a risk factor that may have impact on organization?

a) Management decides to acquire new application software.

b) A new application required by organization is released.

c) Vendor decides to stop supporting existing application.

d) Organization retires old application that is not in use.


Mitigation
Affects
Threat
Resolved by
Exploits
Risk
Vulnerability
Leads to


Four Types of Risk Mitigation
RISK
RISK
RISK
RISK
Accept
Avoid
Transfer
Reduce

8. While auditing risk monitoring process which of the following IS auditor should review FIRST?

a) Risk assessment process

b) Risk management framework

c) Alignment with business risks

d) Annual review of risk register

9. The quantum of risk after enterprise has implemented controls based on risk mitigation plan is:

a) **Accepted risk**

b) **Residual risk**

c) **Inherent risk**

d) **Current risk**

10. Which of the following shall best help in aligning IT risk with enterprise risk?

a) Presenting IT risk results in business terms.

b) Conducting business impact analysis.

c) Making Chief Risk Officer accountable.

d) Align IT strategy with business strategy.

Chapter 2

Administrative Controls of Information Assets

11. The Primary objective of implementing Information security management is to:

a) Ensure reasonable security practices

b) Comply with internal audit requirements

c) Adopt globally recognized standards

d) Protect information assets

12. Which of the following is primary function of information security policies?

a) Align information security practices with strategy

b) Communicate intent of management to stakeholders

c) Perform risk assessment of IT operations and assets

d) Ensure compliance with requirements of standards

13. Information security policies are set of various policies addressing different information systems areas based on the IT infrastructure of organization. Which of the following policy is most common in all organizations?

a) Acceptable use policy

b) BYOD (Bring Your Own Device) policy

c) Data encryption policy

d) Biometric security policy

14. Protecting integrity of data primarily focuses on:

a) Intentional leakage of data

b) Accidental loss of data

c) Accuracy and completeness

d) Data backup procedures

Data integrity refers to the accuracy and consistency (validity) of **data** over its lifecycle.

15. Which of the following is primary reason for periodic review of security policy?

a) Compliance requirements

b) Changes on board of directors'

c) Changes in environment

d) Joining of new employees

16. Which of the following is best evidence indicting support and commitment of senior management for information security initiatives?

a) Directive for adopting global security standard

b) Higher percentage of budget for security projects

c) Assigning responsibilities for security to IT head

d) Information security is on monthly meeting agenda

17. Which of the following is a concern for compliance with information security policy?

a) Decrease in low risk findings in audit report

b) High number of approved and open policy exceptions

c) Security policy is reviewed once in two years

d) Security policy is signed by Chief Information Officer

18. Which of the following is Primary purpose of Information classification?

a) Comply with regulatory requirement

b) Assign owner to information asset

c) Provide appropriate level of protection

d) Reduce costs of data protection

19. Classification of information is primarily based on:

a) Where the information is stored?

b) Who has access to information?

c) What will happen if information is not available?

d) Why attachments to mail are encrypted?

20. Which of the following best helps in classifying the information within organizations?

a) Using minimum classes in classification schema

b) Conducting training on classification schema

c) Labelling all information based on classification schema

d) Determining storage based on classification schema

Chapter 3

Physical and Environmental Controls

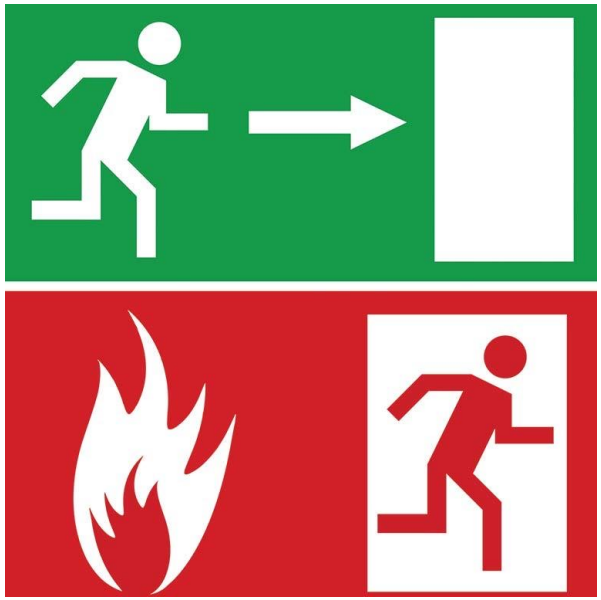
21. Which of the following is first action when a fire detection system raises the alarm?

a) Turn off the air conditioner

b) Determine type of fire

c) Evacuate the facility

d) Turn off power supply



22. Which of the following are most important controls for unmanned data center?

a) Access control for entry and exit for all doors

b) The humidity levels need not be maintained

c) The temperature must be at sub-zero level

d) Halon gas-based fire suppression system

23. Primary purpose of access controlled dead man door, turnstile, mantrap is to:

a) Prevent unauthorized entry

b) Detect perpetrators

c) Meet compliance requirement

d) Reduce cost of guard

24. Which of the following is the main reason for appointing human guards at main entrance of facilities?

a) Address visitors' requirements to visit

b) Issue the access cards to visitors

c) Cost of automation exceeds security budget

d) Deter the unauthorized persons

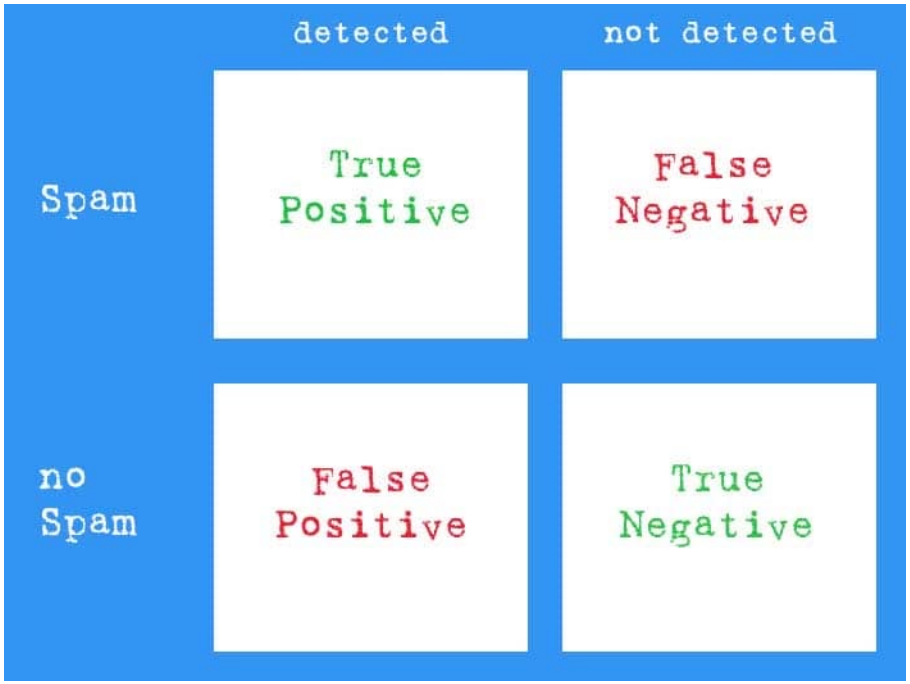
25. Which of the following is a major concern associated with biometric physical access control?

a) High acceptability

b) High false positives

c) High false negatives

d) High cost



26. Which of the following evidence is best to provide assurance on automated environmental controls?

a) Annual maintenance contract with vendor

b) Simulation testing of devices during audit

c) Device implementation report by vendor

d) Documented results of periodic testing

27. What are the problems that may be caused by humidity in an area with electrical devices?

a) High humidity causes excess electricity, and low humidity causes corrosion

b) High humidity causes power fluctuations, and low humidity causes static electricity

c) High humidity causes corrosion, and low humidity causes static electricity

d) High humidity causes corrosion, and low humidity causes power fluctuations.

28. Automated access controls open doors based on access cards, pins, and/or biometric devices and are powered by electricity. Which of the following is the best policy in case of power failure?

a) Keep the door in locked state

b) Open door and appoint guard

c) Find root cause of power failure

d) Arrange for battery backup

29. While selecting site for a data center which of the site is best to be selected?

a) On topmost floor to delay the unauthorized visitor to reach

b) In the basement not easily accessible to perpetrator

c) On ground floor so that users can access it easily

d) On middle floor to strike the balance for above concerns

30. Which of the following is main reason for not allowing mobile devices into data center?

a) Unauthorized changes and access in configuration

b) Prevent photography of data center layout

c) User can provide information to attacker on phone

d) Mobile devices generate wireless communication

Chapter 4

Logical Access Controls

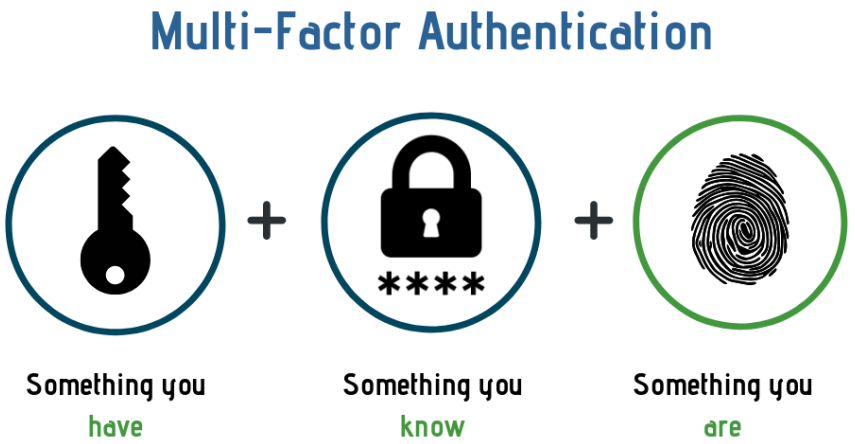
31. Which of the following pair of authentication can be considered as two factors?

a) Password and passphrase

b) Passphrase and PIN

c) Token and access card

d) Access card and PIN



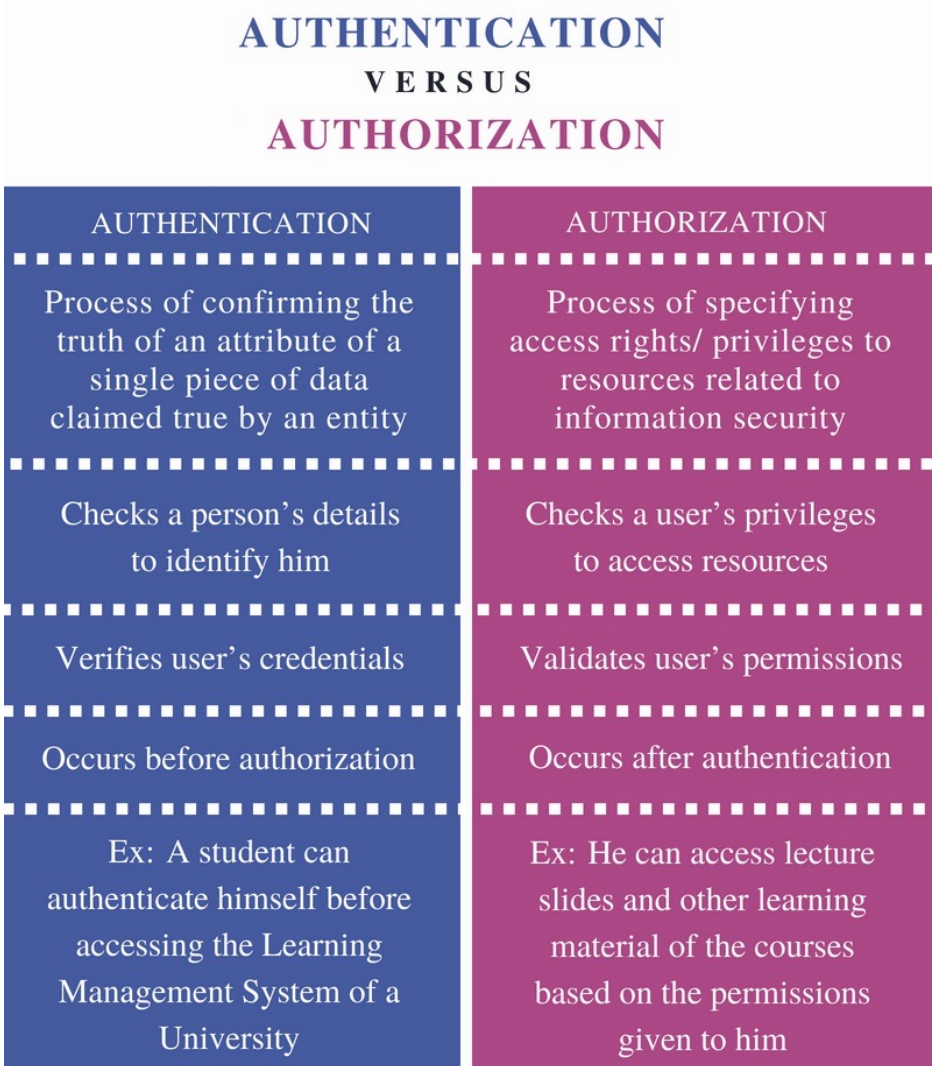
32. Which of the following is primary requirement of granting user access to information asset?

a) Identification

b) Authorization

c) Authentication

d) Need to know



33. Mandatory access controls are those controls that are:

a) Based on global standards

b) Defined by security policy

c) Part of compliance requirements

d) Granted by asset owner

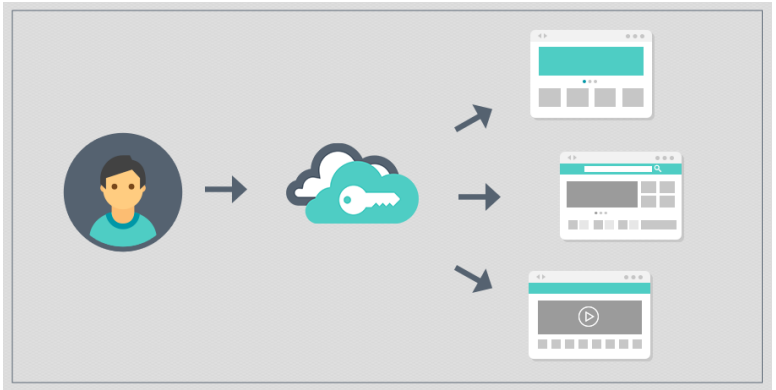
34. Which of the following is a major concern associated with Single-Sign-on?

a) Multiple passwords are noted

b) User may select easy password

c) It is a single point of failure

d) High maintenance cost



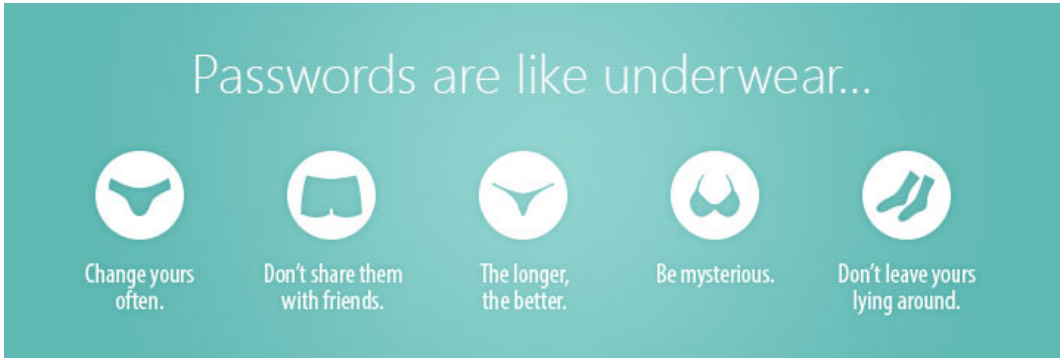
35. Which of the following non-compliance with information security policy is most difficult to detect or get evidence for?

a) Use of removable media

b) Password sharing by user

c) Access to banned web sites

d) Passing information over phone



36. Which of following processes in user access management is most essential to detect errors and omissions resulting in unauthorized or excess accesses to users?

a) **Identification**

b) **Authentication**

c) **Authorization**

d) **User Access Review**

Authentication confirms that users are who they say they are. **Authorization** gives those users permission to access a resource.

User Access Review

- A **user access review** is part of the **user** account management and **access** control process, which involves a periodic **review** of **access** rights for all of an organization's employees and vendors.
- A **user access review** usually includes re-evaluation of: **User** roles. **Access** rights and privileges.

Best practices to conduct a user access review

- Create and update an access management policy
- Create a formalized review procedure
- Implement role-based access control
- Implement the principle of least privilege
- Provide temporary access instead of permanent
- Involve employees and management
- Explain the goals and importance of the review

37. While auditing compliance with password policy, IS auditor observed that configuration of password parameters in system is as per information security policy. Which of the following the auditor should verify?

a) Review enforcement for sample users

b) Verify all assets have same configuration

c) Review log for password configuration

d) Interview users on policy enforcement

Password Parameters

- These profile **parameters** define the minimum requirements for **passwords**, for example, that the **password** must contain at least three special characters.
- You cannot set upper limits for **password** rules.
- For example, in accordance with the usual **password** rules, the users can enter any number of special characters.

- Configure a minimum **password** length.
- Enforce **password** history **policy** with at least 10 previous **passwords** remembered.
- Set a minimum **password** age of 3 days.
- Enable the setting that requires **passwords** to meet complexity **requirements**. ...
- Reset local admin **passwords** every 180 days.

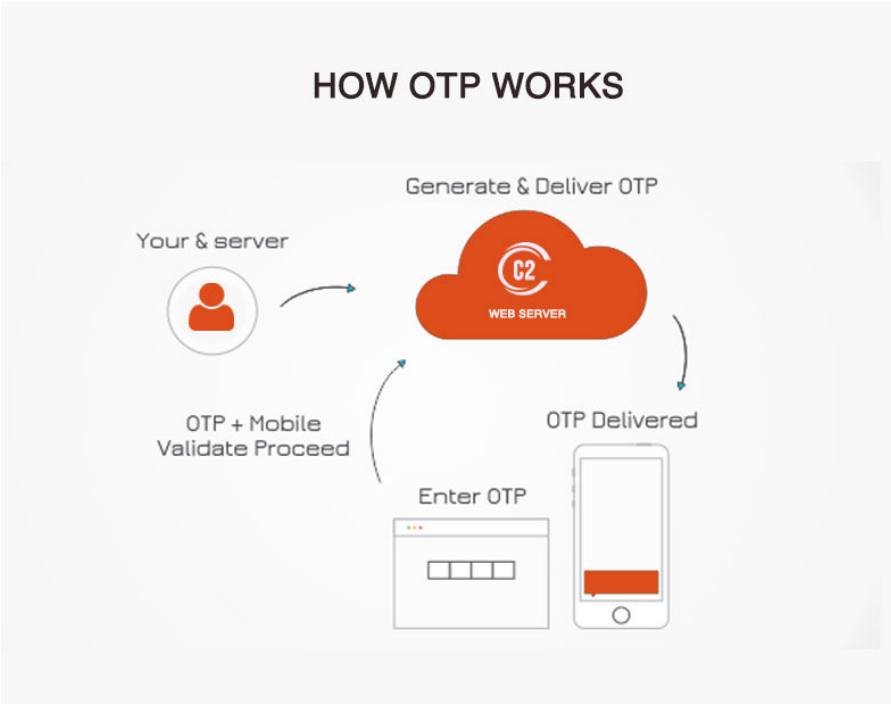
38. One-time password is considered strong because they are:

a) Active for short period

b) Communicated on mobile

c) Unique for each user

d) Unique for session



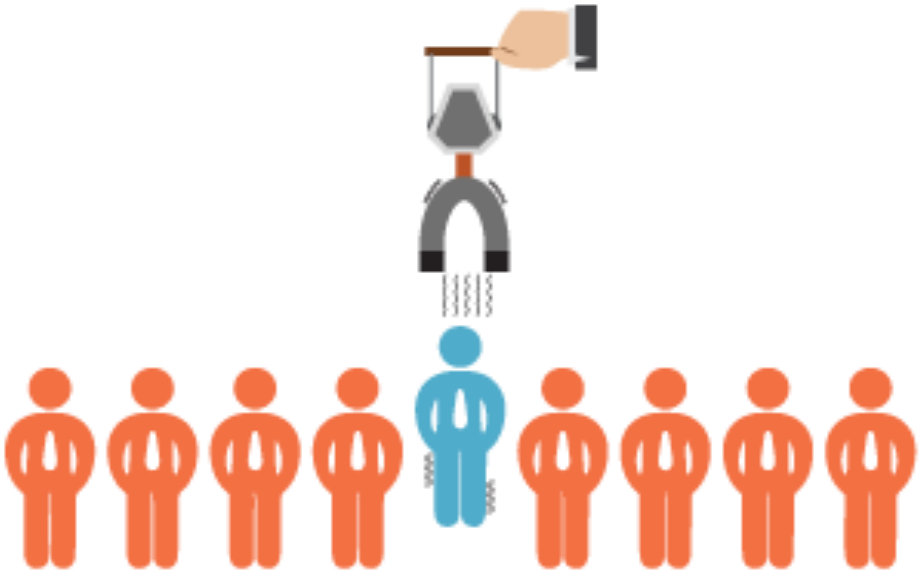
39. Which of the following attack to break the user password is difficult to control?

a) Brute Force

b) Dictionary attack

c) Spoofing

d) Social engineering



40. Which of the following is a primary objective of implementing logical access controls?

a) Identify users on the system

b) Fixing accountability of actions

c) Authorize users based on role

d) Compliance with policy

Protect staff and systems

Prevent intruders and theft

Audit trail and compliance with regulations

Integration across physical and logical access

- **Logical access controls** are tools and protocols used for **identification, authentication, authorization**, and **accountability** in computer information systems.
- Logical access is often needed for remote access of hardware and is often contrasted with the term "physical access", which refers to interactions (such as a lock and key) with hardware in the physical environment, where equipment is stored and used.

Chapter 5
Network Security Controls

41. Which of the following is a method used to gather information about the communication network?

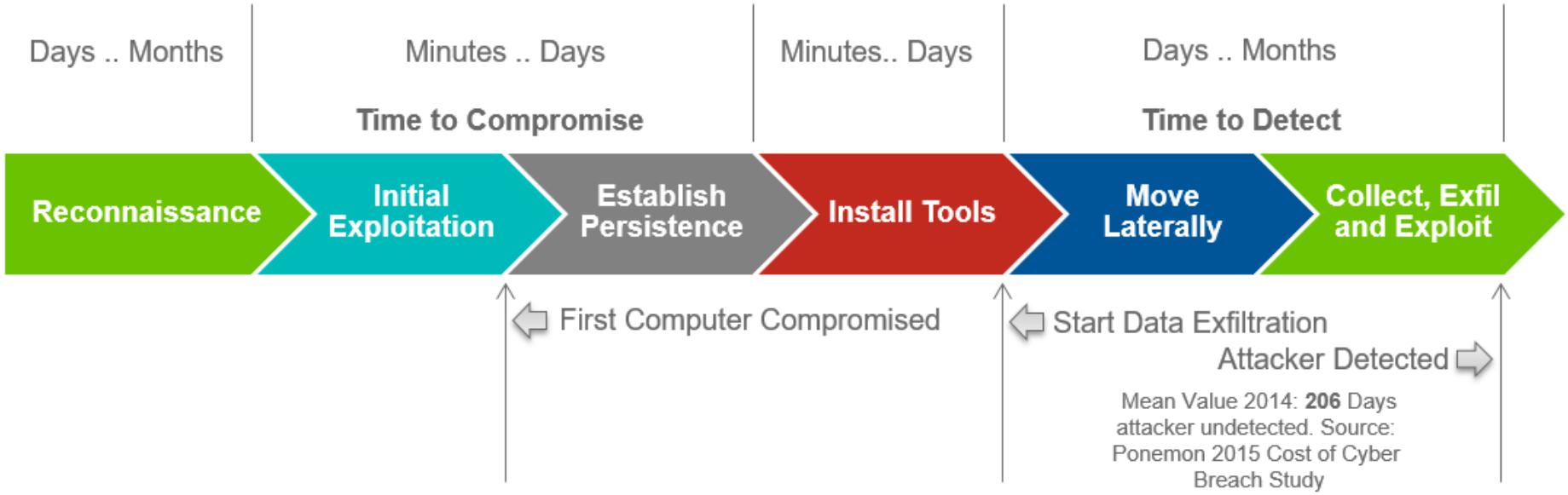
a) Reconnaissance

b) Brute force

c) Eavesdropping

d) Wiretapping

The Six Phases of a Cyber Attack



- To collect as much **information** as possible.
- Collecting **information** and knowing deeply about the target system is known as "**Reconnaissance**".
- This data is the main street for the programmer to hack the target system.
- It involves Footprinting, Enumeration, and Scanning.

42. Message digest helps organization in getting assurance on:

a) Communication delivery

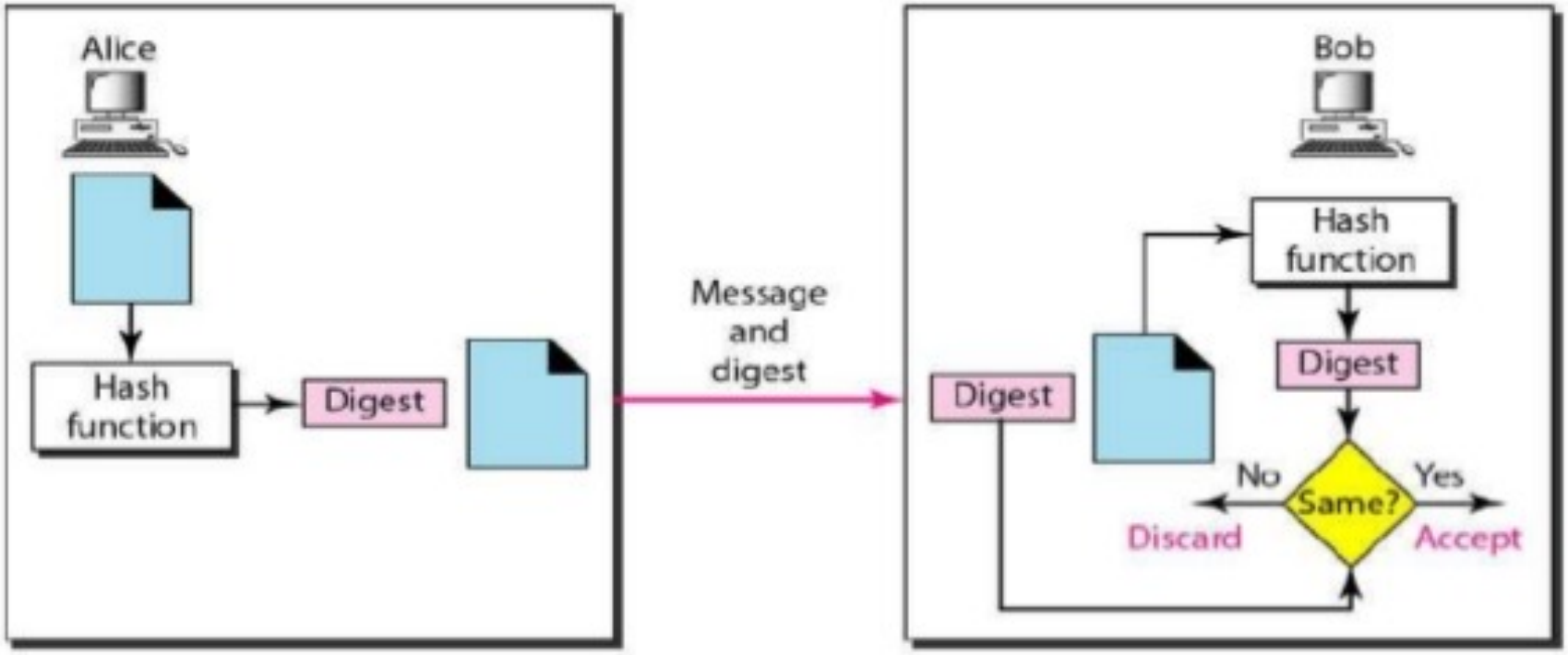
b) Data availability

c) Data integrity

d) Data confidentiality

Message Digest

Different algorithms are used to convert original message into its message digest. The popularly used ones are MD5 or Message Digest 5 (developed by Rivest) a modified version of earlier MD4, MD3 and MD2, while the first one was simply MD, and the SHA (Secure Hash Algorithm) developed by National Institute of Standards and Technology (NISI) in 1993. SHA-I is promoted & prominently used than the MD5 algorithm.



43. While auditing organization's network which of the following control IS auditor must verify first?

a) Encrypted communication

b) Network zoning

c) Firewall configuration

d) Penetration test report

Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.

44. Cryptographic checksum is a network control that:

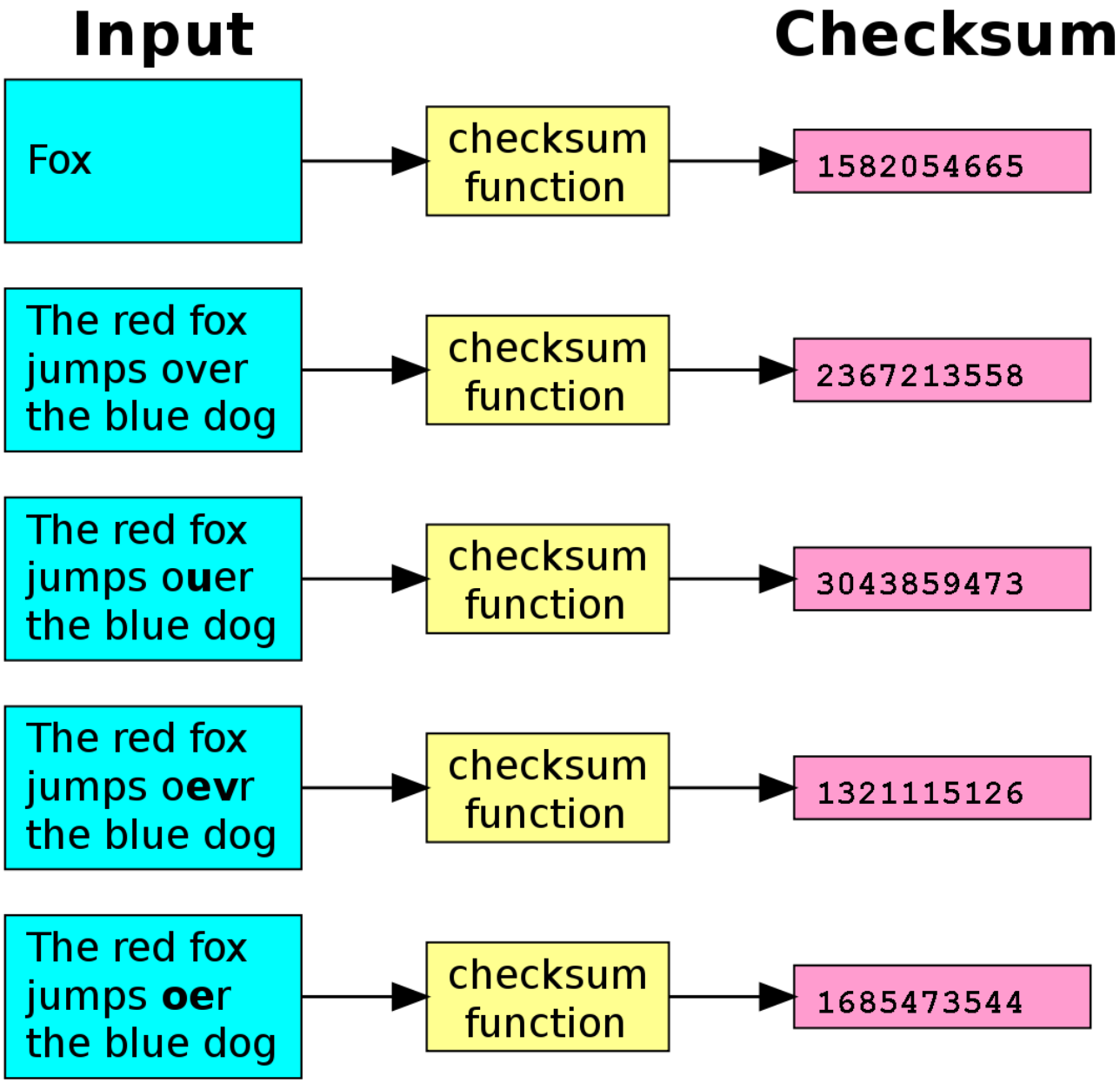
a) Adds a parity bit after adding the data bits.

b) Translates data in a file into a hash value.

c) Transmits the data after encryption.

d) Translates the data into a parity checksum combination.

A **checksum** is a small-sized block of data derived from another block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage. By themselves, checksums are often used to verify data integrity but are not relied upon to verify data authenticity.


Input
Checksum
Fox
checksum function
1582054665
The red fox jumps over the blue dog
checksum function
2367213558
The red fox jumps ouer the blue dog
checksum function
3043859473
The red fox jumps oevr the blue dog
checksum function
1321115126
The red fox jumps oer the blue dog
checksum function
1685473544

45. Primary function of Security Operations Centre (SOC) is to:

a) Define baseline

b) Configure firewall

c) Monitor logs

d) Implement Antivirus

46. The intrusion detection monitoring on a host for data integrity attack by malicious software is a:

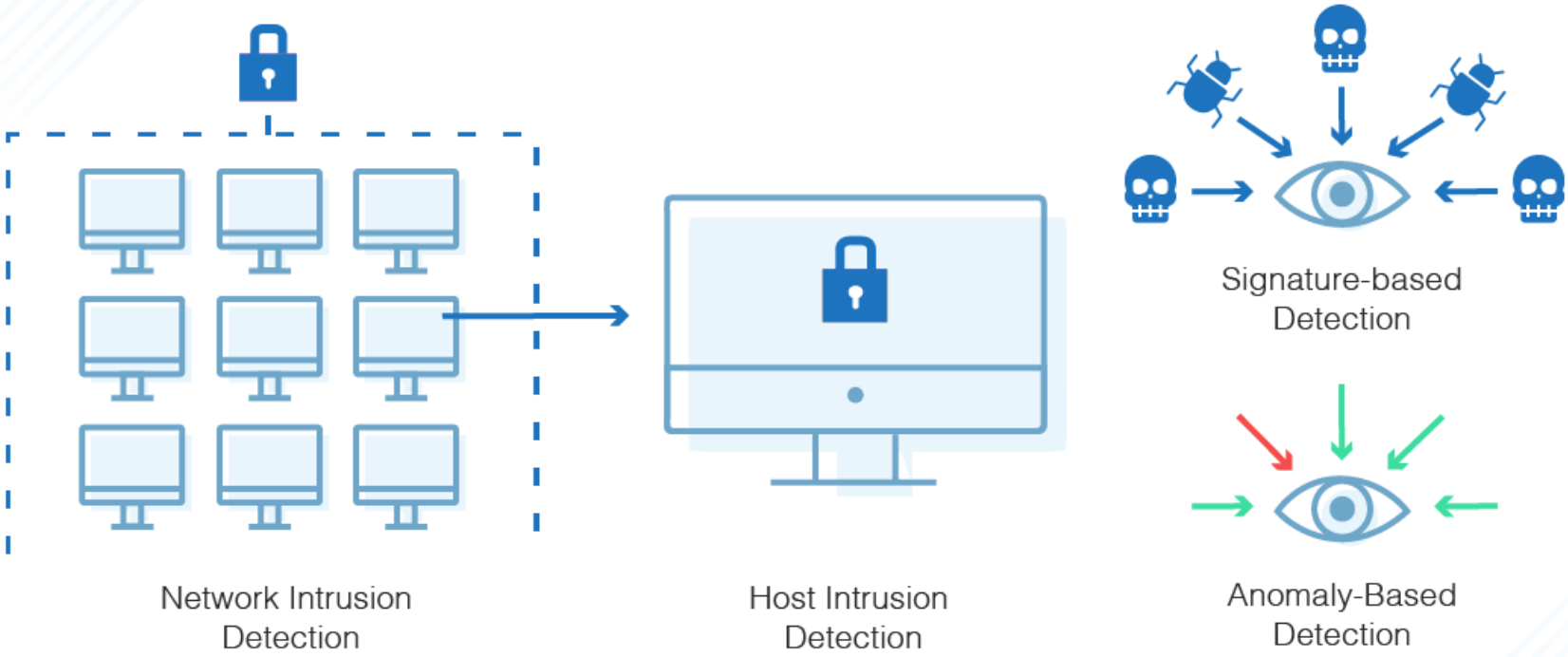
a) Technical control

b) Corrective control

c) Detective Control

d) Preventive Control

What Does an Intrusion Detection System Do?



- An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations.
- Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system (SIEM)

47. Which of the following is most important while performing penetration testing?

a) Maintain secrecy about testing

b) Get consent from affected stakeholders

c) Report to be provided to all users

d) Perform test after office hours

TYPES OF PENETRATION TESTS

NETWORK PENETRATION TEST

- BLACK BOX
- WHITE BOX
- GRAY BOX

WIRELESS PENETRATION TEST

APPLICATION SECURITY TESTING

PHYSICAL PENETRATION TEST

SOCIAL ENGINEERING

- REMOTE
- PHYSICAL

- **Penetration testing**, also called **pen testing** or ethical hacking, is the practice of **testing** a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
- **Penetration testing** can be automated with software applications or performed manually.

48. Most web based application attacks can be prevented by:

a) Input validation

b) Encryption

c) Penetration test

d) Access controls

Input Validation

- Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components.
- Input validation should happen as early as possible in the data flow, preferably as soon as the data is received from the external party.

49. Social engineering attacks can best be prevented by:

a) Intrusion detection system

b) Strong access controls

c) Two factor authentication

d) Awareness training

50. Which of the following is a type of malware that does not use system resources for execution of malicious codes?

a) Virus

b) Logic bomb

c) Trojan Horse

d) Worm

51. Parity bits are a control used to validate:

a) Data authentication

b) Data completeness

c) Data source

d) Data accuracy

52. What is used as a control to detect loss, corruption, or duplication of data?

a) Redundancy check

b) Reasonableness check

c) Hash totals

d) Accuracy check

53. A message digest is a product of which kind of algorithm?

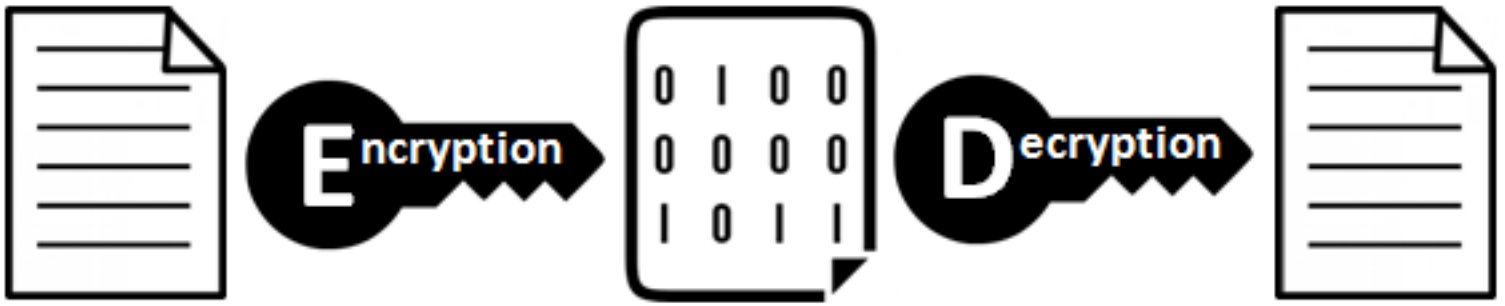
a) Hashing

b) Symmetric

c) Asymmetric

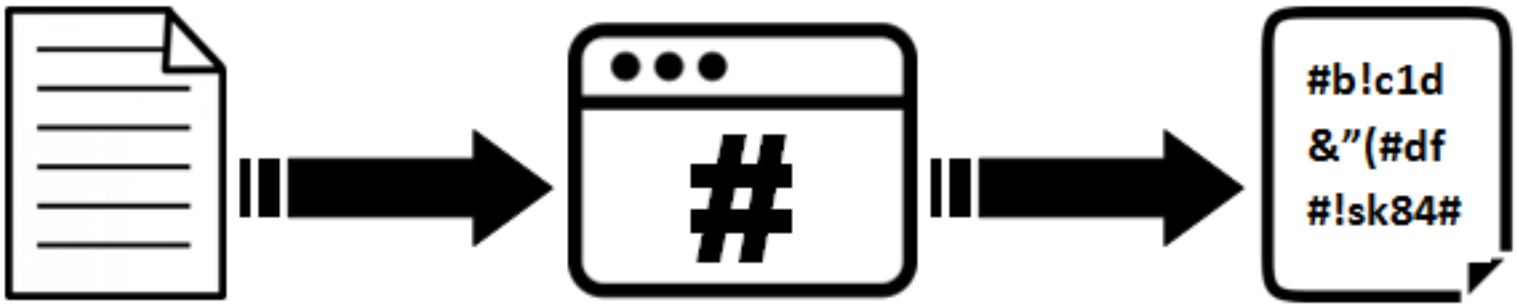
d) Steganography

Encryption & Decryption



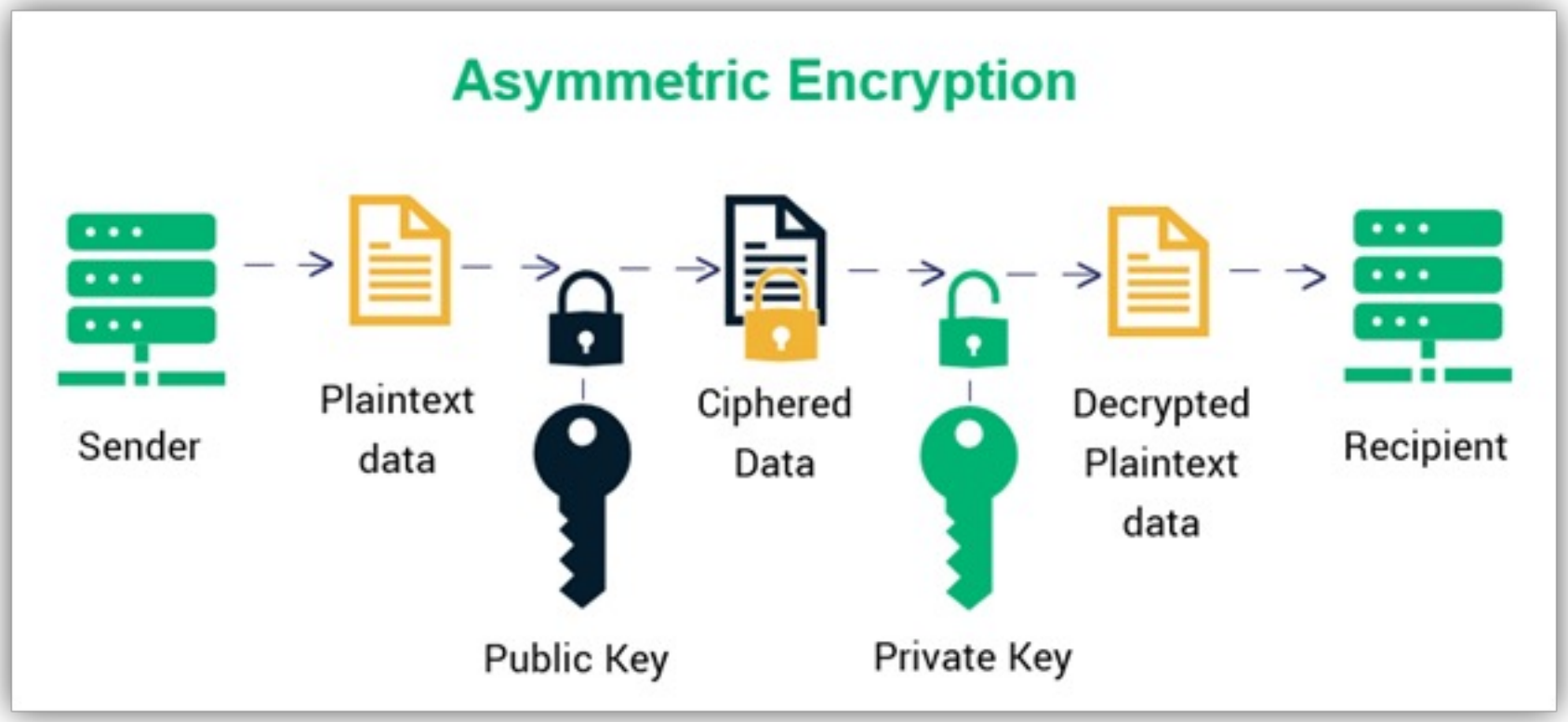
Plain Text | Encrypted Text | Plain Text

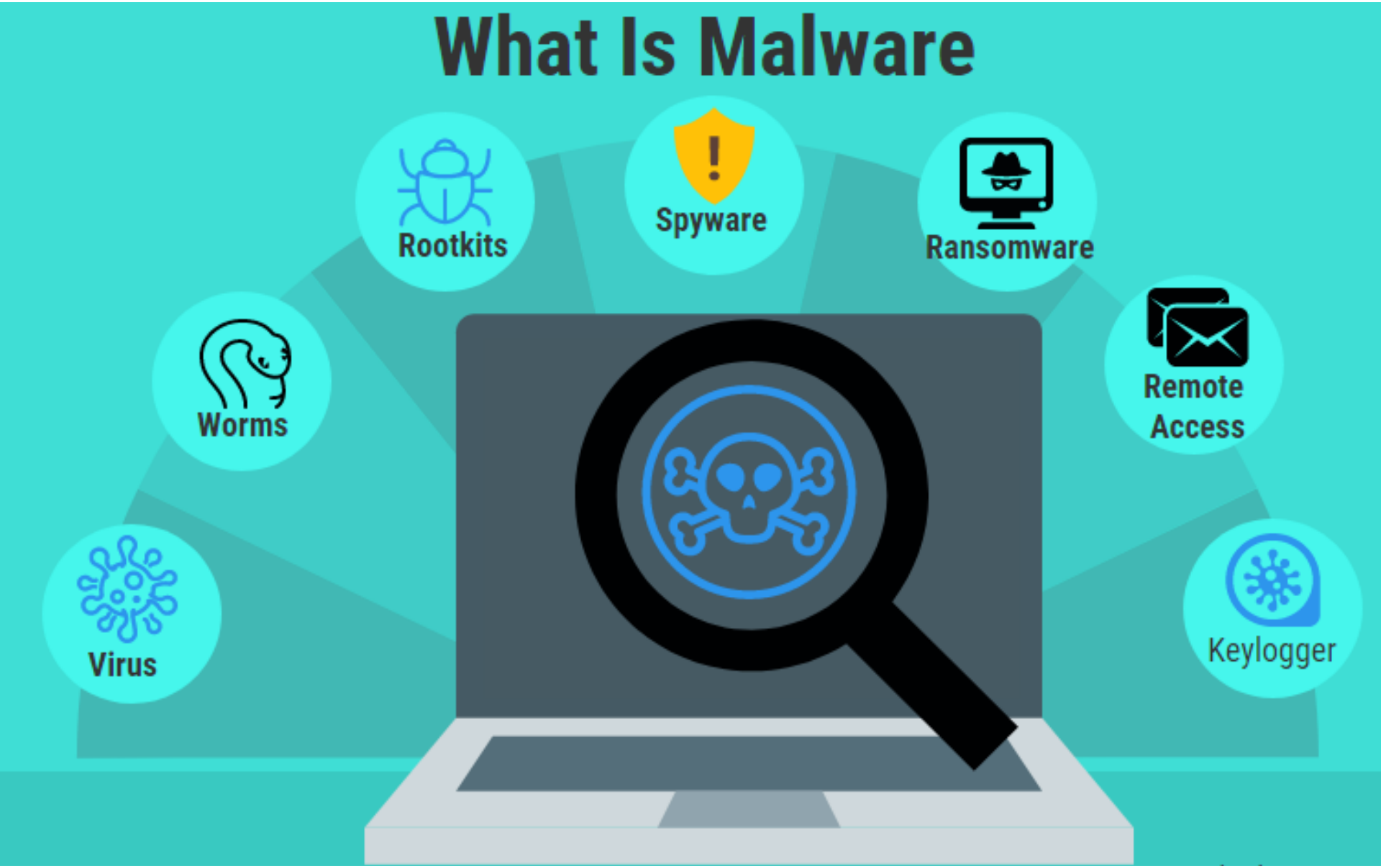
Hashing Algorithm



Plain Text | Hash Function | Hashed Text

Private Key Encryption (Symmetric)


Asymmetric Encryption
Sender
Plaintext data
Public Key
Ciphered Data
Private Key
Decrypted Plaintext data
Recipient


What Is Malware
Rootkits
Spyware
Ransomware
Worms
Remote Access
Virus
Keylogger

- A computer **worm** spreads like a **virus** but is an independent program rather than hidden inside another program.
- A **logic bomb** is a program normally hidden deep in the main computer and set to activate at some point in the future, destroying data.
- A **Trojan horse** (or simply **trojan**) is any malware which misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.
- Computer **worm**s use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time

1	b	11	a	21	c	31	d	41	a	51	b
2	c	12	b	22	a	32	a	42	c	52	c
3	b	13	c	23	a	33	b	43	b	53	a
4	a	14	c	24	a	34	c	44	b	54	a
5	c	15	c	25	b	35	b	45	c	55	?
6	b	16	d	26	d	36	d	46	c	56	?
7	c	17	b	27	c	37	c	47	b		
8	d	18	c	28	b	38	a	48	a		
9	b	19	c	29	d	39	d	49	d		
10	a	20	b	30	a	40	c	50	d		

Case Study:– Data Centre (Cloud) Security

- Silver Cloud Technologies Ltd, a cloud service provider has recently setup a data centre in Bengaluru, India to serve its clientele from Asia and middle east. This data centre is supposed to be a Tier-IV data centre with all the redundancies available for all the facilities. The data centre is setup on a RCC structure with state of the art technology and equipment.
- The data centre is secured with high end physical as well as logical security mechanisms with IT Security policy. IS auditor is appointed to carry out the compliance audit for IT security and submit the report to the BODs. The data centre has an electronic badge system as a part of access control mechanism under which all the employees are allotted a badge having the photo identification as well as a smart card to gain entry inside the data centre as well as high secured zones of the data centre.
- It was also observed that all the access control cards for the visitors are not available in full at the end of the day and there is no periodical reconciliation of these cards. It may be possible that some of the cards are missing and not returned by the visitors.

Case Study:– Data Centre (Cloud) Security

- Apart from this, there are Biometric control devices installed at each critical entry points which are programmed to give access to only those persons who are specifically authorized by the data centre authorization committee. But the retina scan available at the entry point is not effective as the female staffs are not willing to come too close to scanner and hence there are many instances of false rejection cases.
- Whenever, a visitor wants to enter the data centre, a written recommendation letter is asked for. Moreover, a temporary badge is created along with photo identification by registering the person on the spot. In spite of all these strict measures, when a security guard is busy in checking the formalities of one visitor, other visitors can bypass the checking process. It was also observed that no frisking was done at any point of time since inception of the data centre.

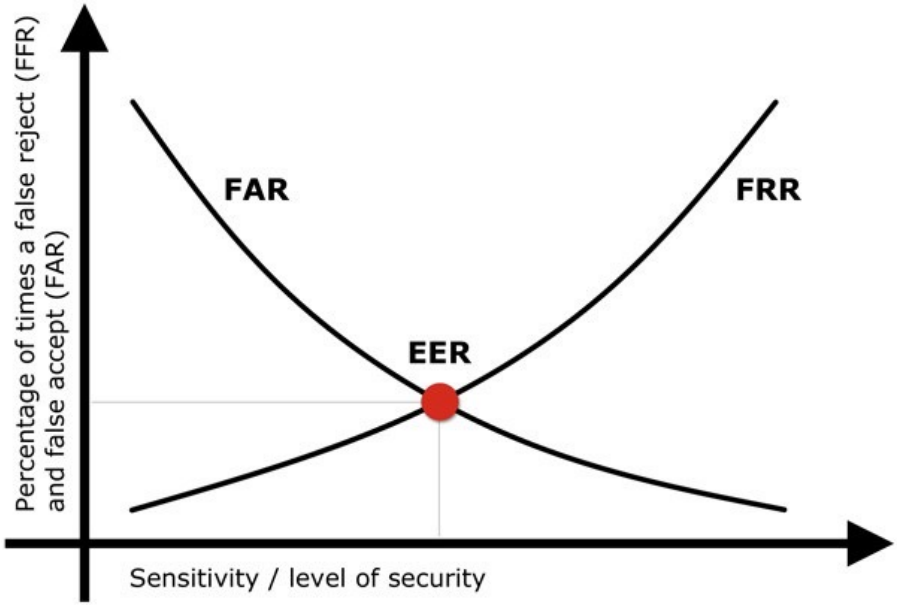
54. Which of the following rate should compulsorily be LOWEST for preventing the unauthorized user gain entry through biometric devices?

a) False Acceptance Rate (FAR)

b) False Rejection Rate (FRR)

c) Equal Error Rate (EER)

d) Average Error Rate (AER)



Biometric Authentication

- Registration or enrolment of the individuals' physical or behavioural characteristics involves capture of information, digitizing and storage of the biometric data.
- Based on the data read by the sensor, the image or digitized data is compared to the stored data to obtain a match. If the match succeeds, authentication is successful. However due to the complexity of data, biometrics suffer from two types of error viz. **False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorized user being wrongfully authenticated as a right user.**
- **Ideally a system should have a low false rejection and low false acceptance rate.** Most biometric systems have sensitivity levels, which can be tuned. The more sensitive a system becomes, FAR drops while FRR increases. Thus, **FRR and FAR tend to inversely related.**
- An overall metric used is the Equal Error Rate (EER), which is the point at which FRR equals FAR. Finger print-based biometric controls are quite popular and widely deployed in data centres.

55. While verifying the security policy on visitors, the auditor will consider it MOST effective when

a) A visitor's photo ID and address proof is scanned and stored for future reference.

b) A visitor is escorted by a specially appointed escort team.

c) A visitor is scanned through X-ray machine and metal detector before entering into the data centre facility.

d) A log of visitor is maintained with signature and contact number.

Page 39: Para 3.4.5

56. IS Auditor finds that the Data Centre has a good number of employees working inside it as well as plenty of servers and network devices. Which of the following fire extinguishers will BEST suit the needs of the data centre?

a) Wet pipe – Water based sprinkler

b) Carbon Dioxide – air based

c) Halon Gas – air based

d) Dry Pipe – Water based sprinkler

CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional & Registered Valuer

Partner : K GOPAL RAO & CO | Chartered Accountants | Mumbai, Chennai, Bengaluru, Hyderabad, Trichy, Madurai & Tiruvallur

Email: gkr@icai.org Blog: www.3spro.blogspot.com

Mobile: 98400 63269 | 98401 63269