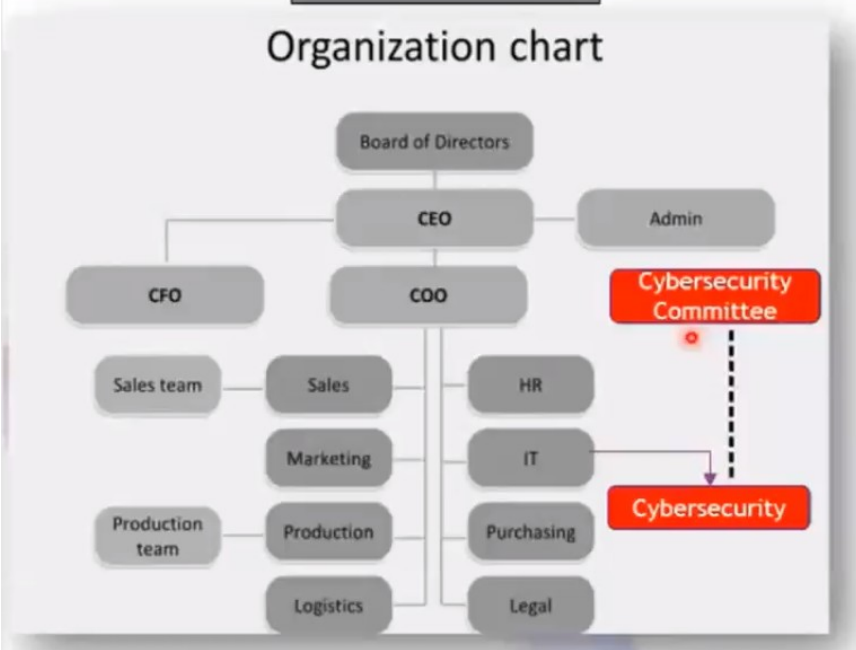
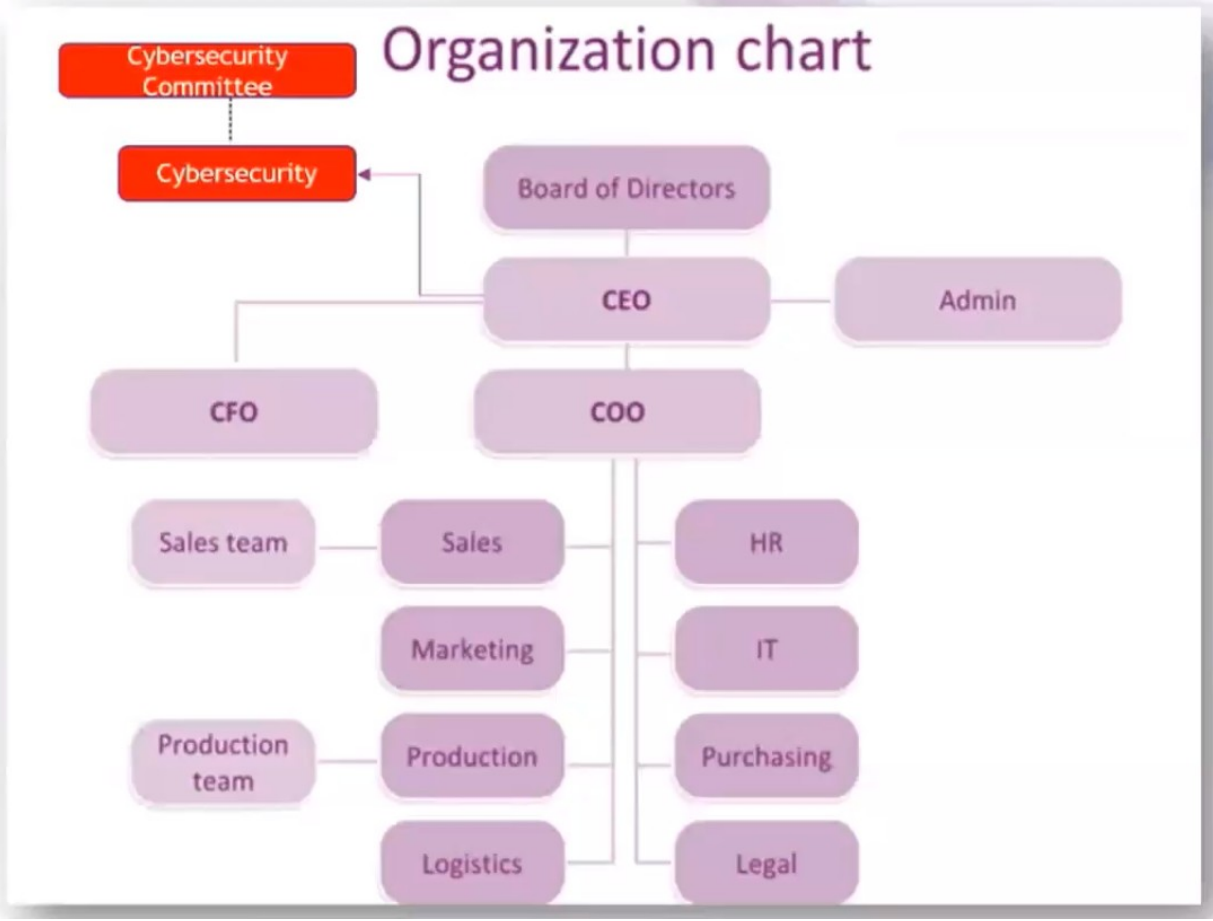
How to achieve this control ?

Prepare a business case to convince the management and take their commitment on the ISO 27001 Implementation

Old School



New School



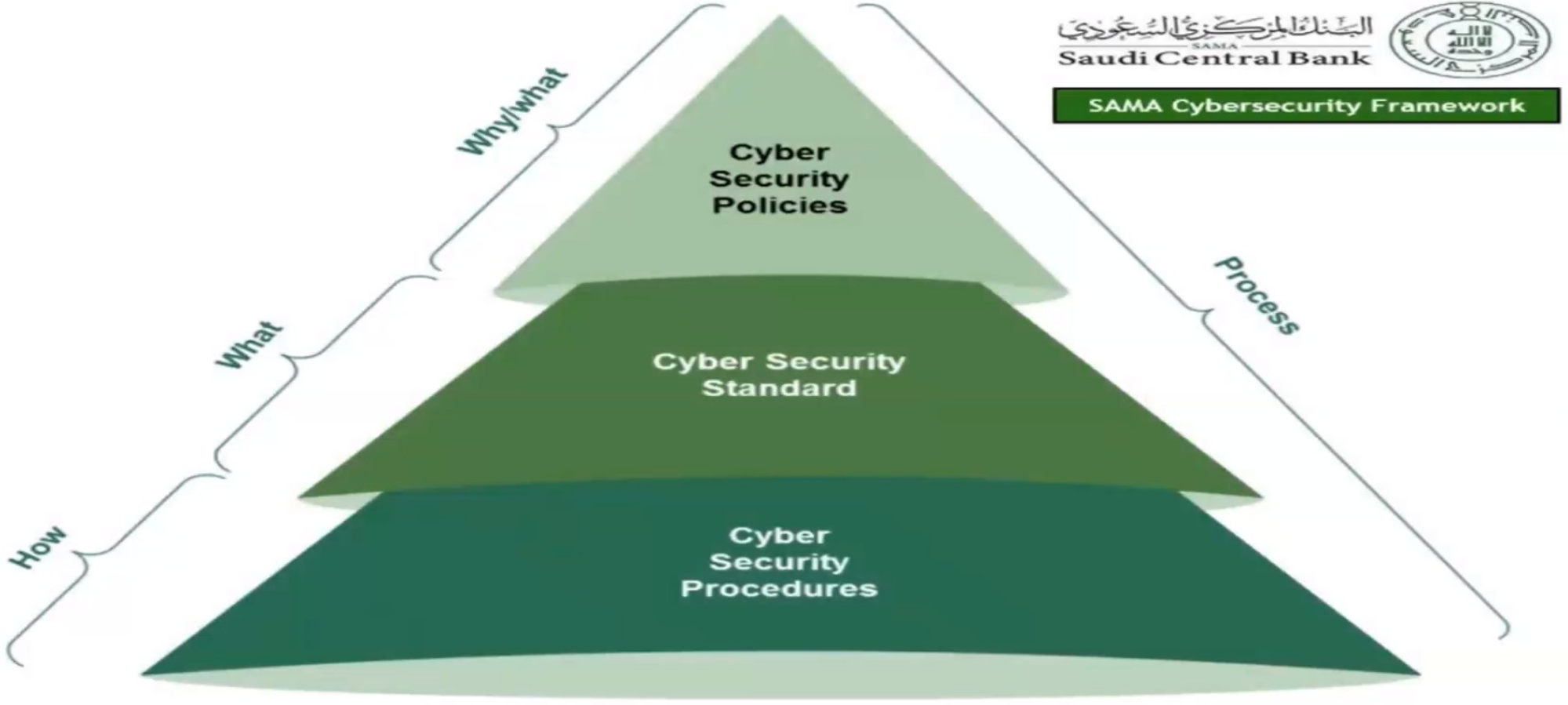


Figure 3 - Cyber Security Documentation Pyramid

NCA - ECC CONTROLS

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

1-2	Cybersecurity Management
Objective	To ensure Authorizing Official's support in implementing and managing cybersecurity programs within the organization as per related laws and regulations
Controls	
1-2-1	A dedicated cybersecurity function (e.g., division, department) must be established within the organization. This function must be independent from the Information Technology/Information Communication and Technology (IT/ICT) functions (as per the Royal Decree number 37140 dated 14/8/1438H). It is highly recommended that this cybersecurity function reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.
1-2-2	The position of cybersecurity function head (e.g., CISO), and related supervisory and critical positions within the function, must be filled with full-time and experienced Saudi cybersecurity professionals.
1-2-3	A cybersecurity steering committee must be established by the Authorizing Official to ensure the support and implementation of the cybersecurity programs and initiatives within the organization. Committee members, roles and responsibilities, and governance framework must be defined, documented and approved. The committee must include the head of the cybersecurity function as one of its members. It is highly recommended that the committee reports directly to the head of the organization or his/her delegate while ensuring that this does not result in a conflict of interest.

SAMA - CYBERSECURITY FRAMEWORK

البنك المركزي السعودي
SAMA
Saudi Central Bank

3.1.1 Cyber Security Governance

Principle

A cyber security governance structure should be defined and implemented, and should be endorsed by the board.

Objective

To direct and control the overall approach to cyber security within the Member Organization.

Control considerations

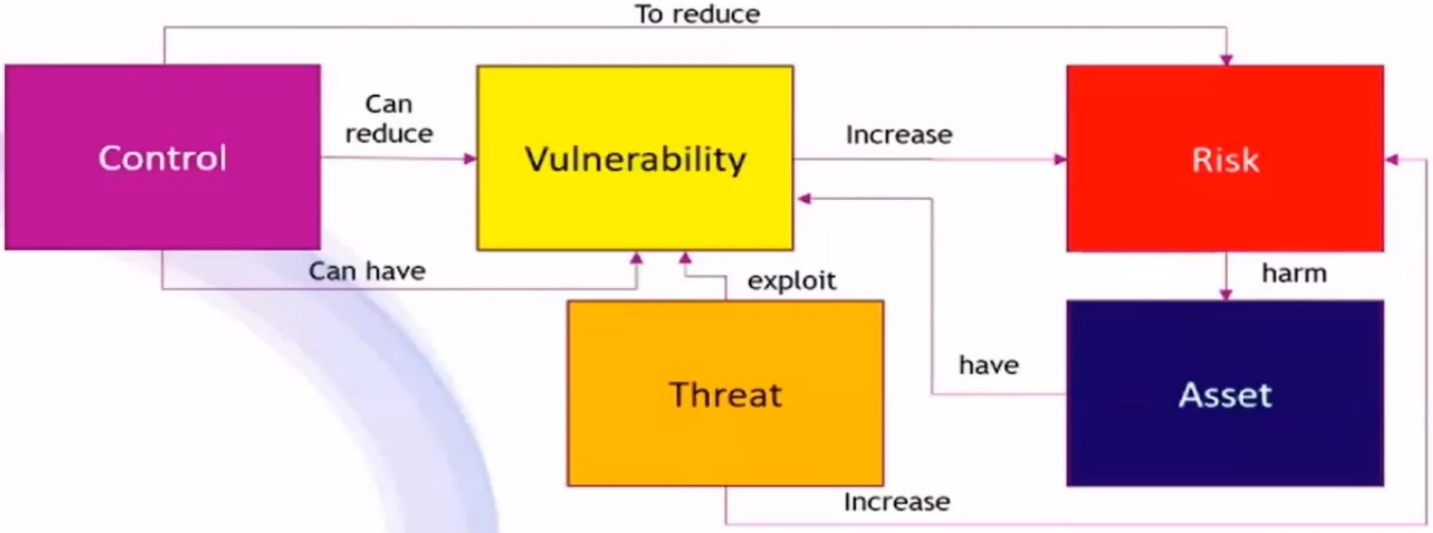
1. A cyber security committee should be established and be mandated by the board.
2. The cyber security committee should be headed by an independent senior manager from a control function.
3. The following positions should be represented in the cyber security committee:
   a. senior managers from all relevant departments (e.g., COO, CIO, compliance officer, heads of relevant business departments);
   b. Chief information security officer (CISO);
   c. Internal audit may attend as an "observer.
4. A cyber security committee charter should be developed, approved and reflect:
   a. committee objectives;
   b. roles and responsibilities;
   c. minimum number of meeting participants;
   d. meeting frequency (minimum on quarterly basis).
5. A cyber security function should be established.
6. The cyber security function should be independent from the information technology function. To avoid any conflict of interest, the cyber security function and information technology function should have separate reporting lines, budgets and staff evaluations.
7. The cyber security function should report directly to the CEO/managing director of the Member Organization or general manager of a control function.
8. A full-time senior manager for the cyber security function, referred to as CISO, should be appointed at senior management level.
9. The Member Organization should :
   a. ensure the CISO has a Saudi nationality;
   b. ensure the CISO is sufficiently qualified;
   c. obtain no objection from SAMA to assign the CISO.
10. The board of the Member Organization should allocate sufficient budget to execute the required cyber security activities.

Relationships Between Information Security Elements

1. Assets and controls can present vulnerabilities that can be exploited by threats.

2. It is the combination of threats and vulnerabilities that can increase the potential effect of the risk.

3. Controls allow the reduction of vulnerabilities. An organization has few alternatives to act against threats. For example, controls can be implemented to provide protection against system intrusions, but it is difficult for an organization to take action to reduce the number of hackers on the internet.



The ISO/IEC 27001 standard classifies security controls in three categories:

Preventive Control

- Discourage or prevent the appearance of problems

Examples:

- Publish an information security policy
- Have a confidentiality agreement signed
- Hire only qualified personnel
- Identify risks coming from third parties
- Segregation of duties

Detective Control

- Search for, detect and identify problems

Examples:

- Monitor and review third-party services
- Monitor the resources used by systems
- Alarm triggers e.g. when sensing fire
- Review of user access rights
- Analysis of audit logs

Corrective Control

- Solve problems found and prevent the recurrence

Examples:

- Technical and legal investigation(forensics) following a security incident
- Activating the business continuity plan after the occurrence of a disaster
- Implementation of patches following the identification of technical vulnerabilities

Risk Management Methodology

You shall have an Enterprise Risk Management Methodology

The information security risk criteria should be established considering the context of the organization and requirements of interested parties and should be defined in accordance with Enterprise Risk Management

Appendix 5: Risk tolerance/treatment table

The table below outlines the level of risk tolerance and treatment depending on the overall level of risk rating:

Risk Ratings	Risk Tolerance / Treatment Required
Extreme Risk	**Unacceptable/No Tolerance** Immediate/Urgent action required Escalate to the Vice-Chancellor and President/Senior Executive Group
High Risk	**Highly Cautious** Within 4 months/Action plan required Requires escalation to Senior Managers and/or applicable Senior Executive member
Medium Risk	**Tolerable/Conservative** Assess the risk and determine if current controls are adequate Management responsibility must be specified
Low Risk	**Acceptable** Manage through routine procedures Unlikely to need specific application of resources.

Appendix 4: Risk rating matrix

All risks within the University are rated using a common scale that assesses:

- The **likelihood** of the University being impacted in that way, and
- the potential **consequences** if the risk were to occur.

The risk rating is determined by combining the consequence and likelihood as shown as follows:

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Extreme
Almost certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

1. Identify security controls to be included in the ISMS.

2. Justify the choice of selected and unselected security controls.

3. Obtain formal approval from the management before the implementation of ISMS.

Bureau Veritas Certification

AEON THANA SINSAP (THAILAND) PUBLIC COMPANY LIMITED

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

The following site is part of the Management System of the above organization

HEAD OFFICE

388 EXCHANGE TOWER, 26TH - 27TH &33RD - 34TH FLOOR, SUKHUMVIT ROAD, KHWAENG KLONGTOEY, KHET KLONGTOEY, BANGKOK 10110 THAILAND

RETAIL FINANCE BUSINESS COMPRISING CREDIT CARD, LOAN, HIRE PURCHASE MOTORCYCLE, WEB BUSINESS SERVICE AND USED CAR HIRE PURCHASE COVERING THE FOLLOWING DEPARTMENTS: FINANCE & ACCOUNTING SHARED SERVICE CENTER, SYSTEM PLANNING, I.T., SYSTEM DEVELOPMENT, MARKETING, CORPORATE GOVERNANCE & CONTROL, BUSINESS CONTROL MANAGEMENT AND LEGAL

STATEMENT OF APPLICABILITY (SOA), VERSION 2.0, EFFECTIVE DATE: NOVEMBER 03, 2014

Certificate No.: TH015313-001 Version: 01 Issue Date: 18-06-2020

The validity of this certificate depends on the validity of the main certificate

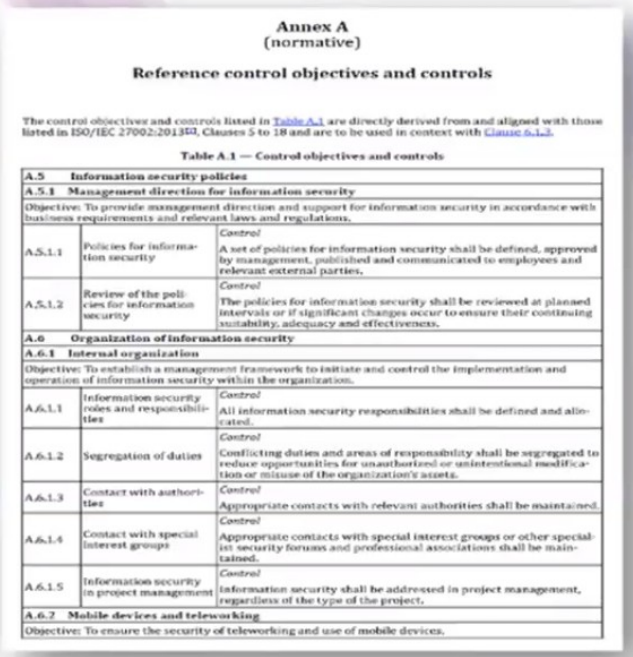
UKAS

Certification Body Address: 5th Floor , 66 Prescot Street, London, E1 8HG, United Kingdom

Local office: Bureau Veritas Certification (Thailand) Ltd. 16th Floor, Bangkok Tower, 2170 New Petchburi Road, Bangkapi, Huaykwang, Bangkok 10310, Thailand

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.

To check this certificate validity please call: +662 670 4800



Annex A
(normative)

Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5	**Information security policies**	
A.5.1	**Management direction for information security**	
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6	**Organization of information security**	
A.6.1	**Internal organization**	
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
A.6.1.5	Information security in project management	*Control* Information security shall be addressed in project management, regardless of the type of the project.
A.6.2	**Mobile devices and teleworking**	
Objective: To ensure the security of teleworking and use of mobile devices.		

The choice of applying a security control should be justified by the conducted information security risk assessment.

Statement of Applicability (SOA) - Example

Security Control#	Security Control name	Control Description	Included /Excluded	Justification for Inclusion or exclusion
A.13.2.3	Electronic Messaging	Information involved in electronic messaging shall be appropriately protected		
A.14.2.1	Secure development Policy	Rules for the development of software and systems shall be established and applied to developments within the organization		

Treatment of problems and nonconformities

Exercise: Determine the proper root cause of the following nonconformity and edit the existing recommendation

Process: Access Management	clause number: A.9.2.1	Site: Bahrain	Type: Minor
Audit criteria:	A formal user registration and de-registration process should be implemented to enable assignment of access rights.		
Description of the observed nonconformity:	In a sample of 10 user registration and revoking requests that have been extracted from the company service hub portal, there are 6 requests have been correctly gone through the whole identity and access management procedure and took the required approvals, and the rest requests have been created without following the procedure and taking the required approvals		
Root Cause:			
Recommendation:	Ensure all user registration and revoking requests are taken the appropriate approvals and following the identity and access management procedure		

	A	B	C	D	E
1	**A6**	**Organization of information security**			
2	**A6.1**	**Internal organization**	**Current Level**	**Description**	**Desired Level**
3	A6.1.1	Information security roles and responsibilities	Initial	ABC will define information security related roles and responsibilities through personnel job descriptions and documented procedures, which will be communicated to all concerned.	Managed
4	A6.1.2	Segregation of duties	Nonexistent	ABC will ensure that job descriptions and procedures are communicated to all concerned, to avoid conflicts and to ensure that access to critical information assets and services are clearly divided among authorized personnel.	Defined
5	A6.1.3	Contact with authorities	Initial	In case of emergency, escalation and reporting procedures will be define to ensure communication with relevant Designations as well as contact with local authorities.	Managed

TIP:
Use Spreadsheet to conduct GAP Analysis

Questions

QUESTION 1
The owner of a system should have the confidence that the system will behave according to its specifications. This is termed as:

A. Integrity
B. Accountability
C. Assurance
D. Availability

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
In a trusted system, all protection mechanisms work together to process sensitive data for many types of uses, and will provide the necessary level of protection per classification level. Assurance looks at the same issues but in more depth and detail. Systems that provide higher levels of assurance have been tested extensively and have had their designs thoroughly inspected, their development stages reviewed, and their technical specifications and test plans evaluated.
In the Trusted Computer System Evaluation Criteria (TCSEC), commonly known as the Orange Book, the lower assurance level ratings look at a system's protection mechanisms and testing results to produce an assurance rating, but the higher assurance level ratings look more at the system design, specifications, development procedures, supporting documentation, and testing results. The protection mechanisms in the higher assurance level systems may not necessarily be much different from those in the lower assurance level systems, but the way they were designed and built is under much more scrutiny. With this extra scrutiny comes higher levels of assurance of the trust that can be put into a system.

Incorrect Answers:
A: Integrity ensures that data is unaltered. This is not what is described in the question.
B: Accountability is a security principle indicating that individuals must be identifiable and must be held responsible for their actions. This is not what is described in the question.
D: Availability ensures reliability and timely access to data and resources to authorized individuals.

QUESTION 2
The US department of Health, Education and Welfare developed a list of fair information practices focused on privacy of individually, personal identifiable information. Which one of the following is incorrect?

A. There must be a way for a person to find out what information about them exists and how it is used.
B. There must be a personal data record-keeping system whose very existence shall be kept secret.
C. There must be a way for a person to prevent information about them, which was obtained for one purpose, from being used or made available for another purpose without their consent.
D. Any organization creating, maintaining, using, or disseminating records of personal identifiable information must ensure reliability of the data for their intended use and must make precautions to prevent misuses of that data.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Fair Information Practice was first developed in the United States in the 1970s by the Department for Health, Education and Welfare (HEW). T Fair Information Practice does not state that there the personal data record-keeping system must be secret.

Incorrect Answers:
A: HEW Fair Information Practices include that there should be mechanisms for individuals to review data about them, to ensure accuracy.
C: HEW Fair Information Practices include
- For all data collected there should be a stated purpose
- Information collected by an individual cannot be disclosed to other organizations or individuals unless specifically authorized by law or by consent of the individual

D: HEW Fair Information Practices include
- Records kept on an individual should be accurate and up to date
- Data should be deleted when it is no longer needed for the stated purpose

QUESTION 3
The typical computer fraudsters are usually persons with which of the following characteristics?

A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
It is easy for people who are placed in position of trust to commit fraud, as they are considered to be trustworthy.

Incorrect Answers:
A: A fraudster might very well have a clean legal record. This in conjunction with a position of trust make him/her hard to detect.
B: It is most typical that a fraudster conspires with other persons as the fraudster usually acts alone.
D: A fraudster can very well follow the accepted norms of society, and this makes him/her harder to detect.

QUESTION 4
The US-EU Safe Harbor process has been created to address which of the following?

A. Integrity of data transferred between U.S. and European companies
B. Confidentiality of data transferred between U.S and European companies
C. Protection of personal data transferred between U.S and European companies
D. Confidentiality of data transferred between European and international companies

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
US-EU Safe Harbor process relates to privacy, that is protection of personal data. The Safe Harbor is a construct that outlines how U.S.-based companies can comply with the EU privacy. The Safe Harbor Privacy Principles states that if a non-European organization wants to do business with a European entity, it will need to adhere to the Safe Harbor requirements if certain types of data will be passed back and forth during business processes

Incorrect Answers:
A: The US-EU Safe Harbor process does not relate to the integrity of the data. It concerns the privacy of the data.
B: The US-EU Safe Harbor process does not relate to the Confidentiality of the data. It concerns the privacy of the data.
D: The US-EU Safe Harbor process does not relate to the Confidentiality of the data. It concerns the privacy of the data.

QUESTION 5
What level of assurance for a digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?

A. Level 1/Class 1
B. Level 2/Class 2
C. Level 3/Class 3
D. Level 4/Class 4

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Users can obtain certificates with various levels of assurance.
Level 1/Class 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). This proves that a human being will reply back if you send an email to that name or email address.

Class 2/Level 2 verify a user's name, address, social security number, and other information against a credit bureau database.

Class 3/Level 3 certificates are available to companies. This level of certificate provides photo identification to accompany the other items of information provided by a level 2 certificate.

Incorrect Answers:
A: Level 1/Class 1 certificates verify electronic mail addresses. They do not verify a user's name, address, social security number, and other information against a credit bureau database.
C: Level 3/Class 3 certificates provide photo identification to accompany the other items of information provided by a level 2 certificate. They do not verify a user's name, address, social security number, and other information against a credit bureau database.
D: Level 4/Class 4 certificates do not verify a user's name, address, social security number, and other information against a credit bureau database.

QUESTION 6
According to Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) there is a requirement to "protect stored cardholder data." Which of the following items cannot be stored by the merchant?

A. Primary Account Number
B. Cardholder Name
C. Expiration Date
D. The Card Validation Code (CVV2)

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) is to "protect stored cardholder data." The public assumes merchants and financial institutions will protect data on payment cards to thwart theft and prevent unauthorized use.
Requirement 3 applies only if cardholder data is stored. Merchants who do not store any cardholder data automatically provide stronger protection by having eliminated a key target for data thieves.
For merchants who have a legitimate business reason to store cardholder data, it is important to understand what data elements PCI DSS allows them to store and what measures they must take to protect those data. To prevent unauthorized storage, only council certified PIN entry devices and payment applications may be used.
PCI DSS compliance is enforced by the major payment card brands who established the PCI DSS and the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS Requirement 3
It details technical guidelines for protecting stored cardholder data. Merchants should develop a data retention and storage policy that strictly limits storage amount and retention time to that which is required for business, legal, and/or regulatory purposes.
Sensitive authentication data must never be stored after authorization – even if this data is encrypted.

- Never store full contents of any track from the card's magnetic stripe or chip (referred to as full track, track, track 1, track 2, or magnetic stripe data). If required for business purposes, the cardholder's name, PAN, expiration date, and service code may be stored as long as they are protected in accordance with PCI DSS requirements.
- Never store the card-validation code (CVV) or value (three- or four-digit number printed on the front or back of a payment card used to validate card-not-present transactions).
- Never store the personal identification number (PIN) or PIN Block. Be sure to mask PAN whenever it is displayed. The first six and last four digits are the maximum number of digits that may be displayed. This requirement does not apply to those authorized with a specific need to see the full PAN, nor does it supersede stricter requirements in place for displays of cardholder data such as in a point-of-sale receipt.

Incorrect Answers:
A: The Primary Account Number can be stored by the merchant according to the PCI Data Storage Guidelines.
B: The Cardholder Name can be stored by the merchant according to the PCI Data Storage Guidelines.
C: The Expiration Date can be stored by the merchant according to the PCI Data Storage Guidelines.

QUESTION 7
Which of the following is NOT a proper component of Media Viability Controls?

A. Storage
B. Writing
C. Handling
D. Marking

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Writing is not a component of media viability controls.
Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.
Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process:

- Marking. All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.
- Handling. Proper handling of the media is important. Some issues with the handling of media include cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.
- Storage. Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:
A: Storage is a media viability control used to protect the viability of data storage media.
C: Handling is a media viability control used to protect the viability of data storage media.
D: Marking is a media viability control used to protect the viability of data storage media.

QUESTION 8
Degaussing is used to clear data from all of the following media except:

A. Floppy Disks
B. Read-Only Media
C. Video Tapes
D. Magnetic Hard Disks

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Atoms and Data
Shon Harris says: "A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussir changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment). "

Degaussing is achieved by passing the magnetic media through a powerful magnet field to rearrange the metallic particles, completely removing any resemblance of the previously recorded signal. Therefore, degaussing will work on any electronic based media such as floppy disks, or hard disks - all of these are examples of electronic storage. However, "read-only media" includes items such as paper printouts and CD-ROM which do not store data in an electronic form or is not magnetic storage. Passing them through a magnet field has no effect on them.

Not all clearing/ purging methods are applicable to all media— for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices. The degree to which information may be recoverable by a sufficiently motivated and capable adversary must not be underestimated or guessed at in ignorance. For the highest-value commercial data, and for all data regulated by government or military classification rules, read and follow the rules and standards.

Incorrect Answers:
A: Floppy Disks can be erased by degaussing.
C: Video Tapes can be erased by degaussing.
D: Magnetic Hard Disks can be erased by degaussing.

QUESTION 9
What is the main issue with media reuse?

A. Degaussing
B. Data remanence
C. Media destruction
D. Purging

Correct Answer: B

Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The main issue with media reuse is data remanence, where residual information still resides on the media.
Data Remanence is the problem of residual information remaining on the media after erasure, which may be subject to restoration by another user, thereby resulting in a loss of confidentiality. Diskettes, hard drives, tapes, and any magnetic or writable media are susceptible to data remanence. Retrieving the bits and pieces of data that have not been thoroughly removed from storage media is a common method of computer forensics, and is often used by law enforcement personnel to preserve evidence and to construct a trail of misuse. Anytime a storage medium is reused (and also when it is discarded), there is the potential for the media's information to be retrieved. Methods must be employed to properly destroy the existing data to ensure that no residual data is available to new users. The "Orange Book" standard recommends that magnetic media be formatted seven times before discard or reuse.

Incorrect Answers:
A: Degaussing is a method used to ensure that there is no residual data left on the media. This is not the main issue with media reuse.
C: Media destruction as the name suggests is the destruction of media. This is not the main issue with media reuse.
D: Purging is another method used to ensure that there is no residual data left on the media. This is not the main issue with media reuse.

QUESTION 10
Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

A. Degaussing
B. Parity Bit Manipulation
C. Zeroization
D. Buffer overflow

Correct Answer: A
Section: Asset Security

Explanation/Reference:
Explanation:
A "Degausser (Otherwise known as a Bulk Eraser) has the main function of reducing to near zero the magnetic flux stored in the magnetized medium. Flux density is measured in Gauss or Tesla. The operation is speedier than overwriting and done in one short operation. This is achieved by subjecting the subject in bulk to a series of fields of alternating polarity and gradually decreasing strength.

Incorrect Answers:
B: Parity has to do with disk error detection, not data removal. A bit or series of bits appended to a character or block of characters to ensure that the information received is the same as the information that was sent.
C: Zeroization involves overwriting data to sanitize it. There is a drawback to this method. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. Degaussing is more effective than overwriting the sectors.
D: This is a detractor. Although many Operating Systems use a disk buffer to temporarily hold data read from disk, its primary purpose has no connection to data removal. An overflow goes outside the constraints defined for the buffer and is a method used by an attacker to attempt access to a system.

QUESTION 11
Which of the following is NOT a media viability control used to protect the viability of data storage media?

A. clearing
B. marking
C. handling
D. storage

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Clearing is not an example of a media viability control used to protect the viability of data storage media.
Media viability controls are implemented to preserve the proper working state of the media, particularly to facilitate the timely and accurate restoration of the system after a failure.
Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process:

- Marking. All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.
- Handling. Proper handling of the media is important. Some issues with the handling of media include cleanliness of the media and the protection from physical damage to the media during transportation to the archive sites.
- Storage. Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust.

Incorrect Answers:
B: Marking is a media viability control used to protect the viability of data storage media.
C: Handling is a media viability control used to protect the viability of data storage media.
D: Storage is a media viability control used to protect the viability of data storage media.

QUESTION 12
An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media or other magnetic media is called:

A. a magnetic field.
B. a degausser.
C. magnetic remanence.
D. magnetic saturation.

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

Incorrect Answers:
A: A magnetic field is not the electrical device described in the question.
C: Magnetic remanence is not the electrical device described in the question.
D: Magnetic saturation is not the electrical device described in the question.

QUESTION 13
What is the most secure way to dispose of information on a CD-ROM?

A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction

Correct Answer: D
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
The information stored on a CDROM is not in electro-magnetic format, so a degausser would be ineffective.
The only way to dispose of information on a CD-ROM is to physically destroy the CD-ROM.

Incorrect Answers:
A: You cannot sanitize read-only media such as a CDROM.
B: Physical damage is not the MOST secure way to dispose of information on a CD-ROM. Data could still be recovered from the undamaged part of the CD-ROM. Only complete destruction of the CD-ROM will suffice.
C: Degaussing does not work on read-only media such as a CDROM.

QUESTION 14
Which of the following refers to the data left on the media after the media has been erased?

A. remanence
B. recovery
C. sticky bits
D. semi-hidden

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data Remanence is the problem of residual information remaining on the media after erasure, which may be subject to restoration by another user, thereby resulting in a loss of confidentiality. Diskettes, hard drives, tapes, and any magnetic or writable media are susceptible to data remanence. Retrieving the bits and pieces of data that have not been thoroughly removed from storage media is a common method of computer forensics, and is often used by law enforcement personnel to preserve evidence and to construct a trail of misuse. Anytime a storage medium is reused (and also when it is discarded), there is the potential for the media's information to be retrieved. Methods must be employed to properly destroy the existing data to ensure that no residual data is available to new users. The "Orange Book" standard recommends that magnetic media be formatted seven times before discard or reuse.

Incorrect Answers:
B: Recovery is not the term that refers to the data left on the media after the media has been erased.
C: Sticky bits is not the term that refers to the data left on the media after the media has been erased.
D: Semi-hidden is not the term that refers to the data left on the media after the media has been erased.

QUESTION 15
What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?

A. Data fiddling
B. Data diddling
C. Salami techniques
D. Trojan horses

Correct Answer: C
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. In this case, the employee has been shaving off pennies from multiple accounts in the hope that no one notices. Shaving pennies from an account is the small crime in this example. However, the cumulative effect of the multiple 'small crimes' is that a larger amount of money is stolen in total.

Incorrect Answers:
A: Data fiddling is not a defined attack type. The term could refer to entering incorrect data in a similar way to data diddling. However, it is not the term used to describe a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account.
B: Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20. This is not what is described in the question.
D: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.

QUESTION 16

Which of the following logical access exposures involvers changing data before, or as it is entered into the computer?

A. Data diddling
B. Salami techniques
C. Trojan horses
D. Viruses

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Data diddling refers to the alteration of existing data. Many times, this modification happens before the data is entered into an application or as soon as it completes processing and is outputted from an application. For instance, if a loan processor is entering information for a customer's loan of $100,000, but instead enters $150,000 and then moves the extra approved money somewhere else, this would be a case of data diddling. Another example is if a cashier enters an amount of $40 into the cash register, but really charges the customer $60 and keeps the extra $20.
This type of crime is extremely common and can be prevented by using appropriate access controls and proper segregation of duties. It will more likely be perpetrated by insiders, who have access to data before it is processed.

Incorrect Answers:
B: Salami techniques: A salami attack is the one in which an attacker commits several small crimes with the hope that the overall larger crime will go unnoticed. This is not what is described in the question.
C: A Trojan Horse is a program that is disguised as another program. This is not what is described in the question.
D: A Virus is a small application or a string of code that infects applications. This is not what is described in the question.

QUESTION 17
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B
Section: Asset Security
Explanation/Reference:
Explanation:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).

There are three general methods of purging media: overwriting, degaussing, and destruction.

There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.

Incorrect Answers:
A: It is not true that clearing completely erases the media or that purging only removes file headers, allowing the recovery of files.
C: Clearing does not involve rewriting the media.
D: It is not true that clearing renders information unrecoverable against a laboratory attack or purging renders information unrecoverable to a keyboard attack.

QUESTION 18
Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

A. Degaussing
B. Overwrite every sector of magnetic media with pattern of 1's and 0's
C. Format magnetic media
D. Delete File allocation table

Correct Answer: A
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
Degaussing is the most effective method out of all the provided choices to erase sensitive data on magnetic media.
A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information.

Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce

the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist.
Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degaussers can destroy drives. The security professional should exercise caution when recommending or using degaussers on media for reuse.

Incorrect Answers:
B: Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There is a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. Degaussing is more effective than overwriting the sectors.
C: Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply removes the pointers to the information.
D: Deleting the File allocation table will not erase all data. The data can be recoverable using software tools.

QUESTION 19
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)

Correct Answer: C
Section: Asset Security
Explanation/Reference:
Explanation:
Secure Electronic Transaction (SET) is a security technology proposed by Visa and MasterCard to allow for more secure credit card transaction possibilities than what is currently available. SET has been waiting in the wings for full implementation and acceptance as a standard for quite some time. Although SET provides an effective way of transmitting credit card information, businesses and users do not see it as efficient because it requires more parties to coordinate their efforts, more software installation and configuration for each entity involved, and more effort and cost than the widely used SSL method.
SET is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet. The following entities would be involved with a SET transaction, which would require each of them to upgrade their software, and possibly their hardware:

- Issuer (cardholder's bank) The financial institution that provides a credit card to the individual.
- Cardholder The individual authorized to use a credit card.
- Merchant The entity providing goods.
- Acquirer (merchant's bank) The financial institution that processes payment cards.
- Payment gateway This processes the merchant payment. It may be an acquirer.

Incorrect Answers:
A: SSH is a network protocol that allows for a secure connection to a remote system. Developed to replace Telnet and other insecure remote shell methods. This is not what is described in the question.
B: S/MIME stands for Secure/Multipurpose Internet Mail Extensions, which outlines how public key cryptography can be used to secure MIME data types. This is not what is described in the question.
D: SSL (Secure Sockets Layer) is most commonly used to Internet connections and e-commerce transactions. It is used instead of SET but is not what is described in the question.

QUESTION 20
In Mandatory Access Control, sensitivity labels attached to object contain what information?

A. The item's classification
B. The item's classification and category set
C. The item's category
D. The item's need to know

Correct Answer: B
Section: Asset Security
Explanation

Explanation/Reference:
Explanation:
A sensitivity label is required for every subject and object when using the Mandatory Access Control (MAC) model. The sensitivity label is made up of a classification and different categories.

Incorrect Answers:
A: The item's classification on its own is incorrect. It has to have a category as well.
C: The item's category on its own is incorrect. It has to have a classification as well.
D: Need-to-know rules are applied by the categories section of the label.

QUESTION 431
Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

A. Palm Scan
B. Hand Geometry
C. Fingerprint
D. Retina scan

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A system that reads a person's retina scans the blood-vessel pattern of the retina on the backside of the eyeball. This pattern has shown to be extremely unique between different people. A camera is used to project a beam inside the eye and capture the pattern and compare it to a reference file recorded previously. Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye. Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:
A: While requiring contact with a surface shared by others, a palm scan is generally considered more acceptable than sharing a surface with other parts of the anatomy. Therefore, this answer is incorrect.
B: A Hand Geometry scan is less accurate and more acceptable than a retina scan. Therefore, this answer is incorrect.
C: A fingerprint scan is more acceptable to users than a retina scan. Users are much more likely to prefer placing their fingers on a fingerprint scanner than looking into a retina scanner. Therefore, this answer is incorrect.

QUESTION 432
Identity Management solutions include such technologies as Directories services, Single Sign-On and Web Access management. There are many reasons for management to choose an identity management solution.

Which of the following is a key management challenge regarding identity management solutions?

A. Increasing the number of points of failures.
B. Users will no longer be able to "recycle" their password for different applications.
C. Costs increase as identity management technologies require significant resources.
D. It must be able to scale to support high volumes of data and peak transaction rates.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identity management is the combination of business process and technology used to manage data on IT systems and applications about users. Managed data includes user objects, identity attributes, security entitlements and authentication factors.
Enterprises manage identity data about two broad kinds of users:
- Insiders: including employees and contractors. They often access multiple internal systems and their identity profiles are relatively complex.
- Outsiders: including customers, partners and vendors. There are normally many more outsiders than insiders.

One of the challenges presented by Identity management is scalability.
Enterprises manage user profile data for large numbers of people. There may be tens of thousands of insiders and hundreds of thousands of outsiders.
Any identity management system used in this environment must scale to support the data volumes and peak transaction rates produced by large user populations.

Incorrect Answers:
A: Increasing the number of points of failures is not key management challenge regarding identity management solutions. There should be no single points of failure but this would be more of a concern for the IT department than management.
B: Users not being able to "recycle" their password for different applications is not a concern for management.
C: A working scalable identity management system is more important to management than the cost. The resource requirement for identity management technologies is not that much when compared to the cost of other systems.

QUESTION 433
When submitting a passphrase for authentication, the passphrase is converted into:

A. a virtual password by the system.
B. a new passphrase by the system.
C. a new passphrase by the encryption technology
D. a real password by the system which can be used forever.

Correct Answer: A
Section: Identity and Access Management
Explanation/Reference:
Explanation:
A passphrase is a sequence of characters that is longer than a password. The user enters this phrase into an application, and the application transforms the value into a virtual password, making the passphrase the length and format that is required by the application. (For example, an application may require your virtual password to be 128 bits to be used as a key with the AES algorithm.) If a user wants to authenticate to an application, such as Pretty Good Privacy (PGP), he types in a passphrase, let's say StickWithMeKidAndYouWillWearDiamonds. The application converts this phrase into a virtual password that is used for the actual authentication.
A passphrase is more secure than a password because it is longer, and thus harder to obtain by an attacker. In many cases, the user is more likely to remember a passphrase than a password.

Incorrect Answers:
B: The passphrase is not converted into a new passphrase by the system.
C: The passphrase is not converted into a new passphrase by the encryption technology.
D: The passphrase is not converted into a real password by the system which can be used forever.

QUESTION 434
Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

A. Extensible Authentication Protocol
B. Challenge Handshake Authentication Protocol
C. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Extensible Authentication Protocol (EAP) is defined as:
A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

The Extensible Authentication Protocol (EAP) is a protocol for wireless networks that expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards,

certificates, one-time passwords, and public key encryption authentication.

Incorrect Answers:
B: The definition in the question does not describe Challenge Handshake Authentication Protocol.
C: The definition in the question does not describe Remote Authentication Dial-In User Service.
D: The definition in the question does not describe Multilevel Authentication Protocol.

QUESTION 435
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

A. 100 subjects per minute.
B. 25 subjects per minute.
C. 10 subjects per minute.
D. 50 subjects per minute.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
In addition to the accuracy of the biometric systems, there are other factors that must also be considered. These factors include the enrollment time, the throughput rate, and acceptability.
The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a system. Acceptable throughput rates are in the range of 10 subjects per minute.

Incorrect Answers:
A: 100 subjects per minute is just over half a second per user. This is way faster than is necessary.
B: 25 subjects per minute is less than 3 seconds per user. This is faster than necessary as people using a biometric scanner would not use it that quickly.
D: 50 subjects per minute is just over one second per user. This is faster than necessary as people using a biometric scanner would not use it that quickly.

QUESTION 436
Which of the following biometric parameters are better suited for authentication use over a long period of time?

A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Of the answers given, the iris is the least likely to change over a long period of time which makes the iris pattern better suited for authentication use over a long period of time.
The iris is the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas, and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the information gathered during the enrollment phase. Of the biometric systems, iris scans are the most accurate. The iris remains constant through adulthood, which reduces the type of errors that can happen during the authentication process.

Incorrect Answers:
B: A person's voice pattern is less suited for authentication use over a long period of time because the voice pattern can change over time.
C: A person's signature is less suited for authentication use over a long period of time because the signature can change over time.
D: A person's retina pattern is less suited for authentication use over a long period of time because the retina pattern can change over time and can be changed by illnesses such as Diabetes.

QUESTION 437
Which of the following is NOT a disadvantage of Single Sign On (SSO)?

A. Support for all major operating system environment is difficult
B. The cost associated with SSO development can be significant
C. SSO could be single point of failure and total compromise of an organization asset
D. SSO improves an administrator's ability to manage user's account and authorization to all associated system

Correct Answer: D
Section: Identity and Access Management

Explanation:
Single sign-on (SSO) gives the administrator the ability to streamline user accounts and better control access rights. It, therefore, improves an administrator's ability to manage users and user configurations to all associated systems.

Incorrect Answers:
A: A disadvantage of SSO is that insufficient software solutions accommodate all major operating system environments. A mix of solutions must, therefore, be adapted to the enterprise's IT architecture and strategic direction.
B: A disadvantage of SSO is that considerable interface development and maintenance may be required, which could be costly.
C: SSO could be single point of failure and total compromise of an organization asset. This means that that if an attacker uncovers a credential set, the attacker would have access to every resource within the environment that the compromised account has access to.

QUESTION 439
In the context of Biometric authentication, there is a quick way to compare the accuracy of devices. In general, the devices that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

A. the CER is used.
B. the FRR is used
C. the FAR is used
D. the FER is used

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
There are three main performance measures in biometrics. These measures are as follows:
- False Rejection Rate (FRR) or Type I Error. The percentage of valid subjects that are falsely rejected.
- False Acceptance Rate (FAR) or Type II Error. The percentage of invalid subjects that are falsely accepted.
- Crossover Error Rate (CER). The percent in which the False Rejection Rate equals the False Acceptance Rate.

Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, such as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase. Thus, to have a valid measure of the system performance, the CER is used.

Incorrect Answers:
B: FRR is the percentage of valid subjects that are falsely rejected. It is not used to compare accuracy of biometric devices.
C: FAR is the percentage of invalid subjects that are falsely accepted. It is not used to compare accuracy of biometric devices.
D: FER is not used to compare accuracy of biometric devices.

QUESTION 440

Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan
B. Fingerprint scan
C. Hand geometry
D. Signature recognition

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Acceptability in terms of biometric systems refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems may be the exchange of body fluids on the eyepiece or the feeling that a retinal scan could be harmful to the eye. Another concern would be the retinal pattern that could reveal changes in a person's health, such as diabetes or high blood pressure.

Incorrect Answers:
A: While requiring contact with a surface shared by others, a fingerprint scan is generally considered more acceptable than sharing a surface with other parts of the anatomy.
B: While requiring contact with a surface shared by others, a hand geometry scan is generally considered more acceptable than sharing a surface with other parts of the anatomy.
C: A signature does not involve contact with a surface shared by others and is therefore more acceptable than other biometric methods.

QUESTION 442
Which of the following does NOT apply to system-generated passwords?

A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Passwords that are generated by a system or a password generation tool are robust passwords in that they will contain a mix of uppercase characters, lowercase characters, numbers and non-alphanumeric characters.
One of the benefits of system-generated passwords is that they are LESS (not more) vulnerable to brute force and dictionary attacks.

Incorrect Answers:

A: It is true that system-generated passwords are harder to remember for users. This is due to the complexity of the password.
B: It is true that if the password-generating algorithm gets to be known, the entire system is in jeopardy. This is because it would be possible to crack the passwords by using the algorithm used to create the passwords.
D: It is true that system-generated passwords are harder to guess for attackers. This is due to the complexity of the password.

QUESTION 443
What is the MOST critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements
C. Accuracy
D. Scalability

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Biometrics are based on the Type 3 authentication mechanism — something you are. Biometrics are defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.
The most critical characteristic of a biometric identifying system (or any other identification and authentication system) is the accuracy of the system. The system needs to ensure that the identification of the person is correct.

Incorrect Answers:
A: The perceived intrusiveness of a biometric system is an important consideration. Users will not be happy to use a system which is perceived to be too intrusive. However, this is not as critical as the accuracy of the system.
B: The storage requirement of a biometric system is not an important consideration. Storage is cheap nowadays and biometric data does not require much storage space.
D: The scalability of a biometric system could be an important consideration if the company intends to expand in the future although most biometric systems are easily scalable. However, this is not as critical as the accuracy of the system.

QUESTION 444
What is considered the MOST important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
A Type II Error occurs when the system accepts impostors who should be rejected. This type of error is the most dangerous type, and therefore the most important to avoid.

Incorrect Answers:
A: A Type I Error is when a biometric system rejects an authorized individual. It is not as dangerous as a Type II Error, and therefore not the most important to avoid.
C: Combined Error Rate is not a valid type of biometric error.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate. It is the most important measurement when determining the system's accuracy.

QUESTION 445
How can an individual/person BEST be identified or authenticated to prevent local masquerading attacks?

A. User Id and password
B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Masquerading is the term used when one user pretends to be another user. Strong authentication is the best defense against this.
Authentication is based on the following three factor types:

- Type 1. Something you know, such as a PIN or password
- Type 2. Something you have, such as an ATM card or smart card
- Type 3. Something you are (physically), such as a fingerprint or retina scan

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification.
A biometric authentication such as a fingerprint cannot be imitated which makes biometrics the best defense against masquerading attacks.

Incorrect Answers:
A: A user Id and password can be guessed by an attacker. This is not the best identification and authentication method to prevent local masquerading attacks.
B: A smart card can be stolen and the PIN guessed by an attacker. This is not the best identification and authentication method to prevent local masquerading attacks.
C: Two-factor authentication is more secure than other methods but still less secure than biometrics. Two-factor authentication could comprise of "something you have" and "something you know". The "something you have" such as a smart card could be stolen by an attacker and the "something you know" such as a PIN could be guessed. This is not the best identification and authentication method to prevent local masquerading attacks.

QUESTION 451
Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these items listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

A. Multi-party authentication
B. Two-factor authentication
C. Mandatory authentication
D. Discretionary authentication

Correct Answer: B
Section: Identity and Access Management

Explanation/Reference:
Explanation:
Two-factor authentication provides identification of users via the combination of two different components, which could be something that the user knows, something that the user possesses or something that is inseparable from the user.

Incorrect Answers:
A: Multi-party authentication is not a valid term.
C: Mandatory authentication is not a valid term.
D: Discretionary authentication is not a valid term.

QUESTION 452
Legacy single sign on (SSO) is:

A. Technology to allow users to authenticate to every application by entering the same user ID and password each time, thus having to remember only a single password.
B. Technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals.
C. A mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
D. Another way of referring to SESAME and KryptoKnight, now that Kerberos is the de-facto industry standard single sign on mechanism.

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Legacy single sign on (SSO) is a mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
An SSO solution may provide a bottleneck or single point of failure. If the SSO server goes down, users are unable to access network resources. This is why it's a good idea to have some type of redundancy or fail-over technology in place.

Incorrect Answers:
A: Legacy single sign on (SSO) enables users to sign on once; they do not have to sign on to every application.
B: Legacy single sign on (SSO) is not technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals. This can be done with password synchronization.
D: Legacy single sign on (SSO) is not another way of referring to SESAME and KryptoKnight.

QUESTION 453
Which type of password token involves time synchronization?

A. Static password tokens
B. Synchronous dynamic password tokens
C. Asynchronous dynamic password tokens
D. Challenge-response tokens

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Synchronous dynamic tokens make use of time or counters to synchronize a displayed token code with the code expected by the authentication server. Hence, the codes are synchronized.

Incorrect Answers:
A: Static passwords are reusable passwords that may or may not expire, and are normally user generated.
C: Asynchronous dynamic tokens are not synchronized with a central server.
D: Challenge-response tokens are asynchronous dynamic password tokens.

QUESTION 454
Which of the following would describe a type of biometric error refers to as FASLE rejection rate?

A. Type I error
B. Type II error
C. Type III error
D. CER error

Correct Answer: A
Section: Identity and Access Management

Explanation:
A Type I error, or false rejection rate, is when a biometric system rejects an authorized individual.

Incorrect Answers:
B: A Type II error, or false acceptance rate, is when the system accepts impostors who should be rejected.
C: A Type III error does not exist in biometrics.
D: The crossover error rate (CER) is a percentage that signifies the point at which the false rejection rate equals the false acceptance rate.

QUESTION 455
Which of the following statements pertaining to biometrics is FALSE?

A. Increased system sensitivity can cause a higher false rejection rate
B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
C. False acceptance rate is also known as Type II error.
D. Biometrics are based on the Type 2 authentication mechanism.

Correct Answer: D
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Type 2 authentication is based on something you have, like a token. Biometrics for part of Type 3 authentication, which is based on something you are. Something you are refers to an individual's physical traits.

Incorrect Answers:
A, B, C: These options are all TRUE with regards to biometrics.

QUESTION 456
Which of the following statements pertaining to Kerberos is TRUE?

A. Kerberos does not address availability

B. Kerberos does not address integrity

C. Kerberos does not make use of Symmetric Keys

D. Kerberos cannot address confidentiality of information

Correct Answer: A
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Kerberos addresses the confidentiality and integrity of information. It does not address availability.

Incorrect Answers:
B: Kerberos does address integrity.
C: Kerberos does make use of Symmetric Keys.
D: Kerberos does address confidentiality of information.

QUESTION 457
Which of the following BEST ensures accountability of users for the actions taken within a system or domain?

A. Identification
B. Authentication
C. Authorization
D. Credentials

Correct Answer: B
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
Identification and authentication are the keystones of most access control systems. Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system. Authentication is verification that the user's claimed identity is valid and is usually implemented through a user password at log-on time.

To 'ensure' accountability, the user must prove that they are who they say they are. This is the function of authentication. Therefore, authentication best ensures accountability of users for the actions taken within a system or domain.

Incorrect Answers:
A: Identification is the user saying who they are. However, to ensure accountability, you need authentication to prove that they are who they say they are.
C: Authorization is the rights and permissions granted to an individual which enable access to a computer resource. This does not ensure accountability because it does not ensure that the user accessing the system is who they say they are.
D: Credentials are the user's username and password combination. However, authentication is the process of validating the credentials. Credentials alone (without validation/authentication) do not ensure that the user accessing the system is who they say they are.

QUESTION 459
Which of the following biometric devices offers the LOWEST CER?

A. Keystroke dynamics
B. Voice verification
C. Iris scan
D. Fingerprint

Correct Answer: C
Section: Identity and Access Management
Explanation

Explanation/Reference:
Explanation:
According to the SANS Institute, an Iris scan has a lower CER than keystroke dynamics, voice verification, and fingerprint.

Incorrect Answers:
A, B, D: According to the SANS Institute, keystroke dynamics, voice verification, and fingerprint has a higher CER than iris scan.

THANKS!