Question 1

Explain why it is important that development of a security system is done in a top-down manner rather than bottom-up.

1. A top-down approach manner would allow the development of the security system to be more aligned with the long-term business goals of the company.
2. The approach would be more cost effective as money is spent where it is needed the most. The project would be able to receive funding support from top management.

Question 2

Explain the primary difference between standards and procedures.

Policies (WHY)

* Policies define what an organisation needs. (WHY)

Standards (WHAT)

* Standards take this a step further and define the requirements.
* Standards provide the agreement that provides interoperability within the organisation through the use of common protocols.
* Standards simplify the operation of the security controls within the company and increase efficiency

Procedures (HOW)

* The step-by-step instructions in support of the policies, the standards, the guidelines, the baselines.
* Indicates how the policy will be implemented and who does what to accomplish the task.
* More clarity and understanding to the operation, to effectively support the policy on a consistent basis.

Question 3

Give an example of a user-based vulnerability and related threat that could compromise confidentiality.

Vulnerability: Lack of security awareness training on phishing for the employees

Threat: Hacker sends a phishing emails to the users to hack the system

REFER TO OTHER DOC

Question 4

A financial institution is planing to develop an information system in order to provide online banking services to its customers via desktop computers and mobile devices. Describe your interpretation of the security goal Integrity in this specific context by listing three (3) requirements of the information system to be developed.

3 Integrity requirements:

* Prevent unauthorised modifications
* Prevent improper modification
* Ensure information is consistent and reliable

1. Authorised access only an authorised customer or authorised supervisor in the bank can have access to information of customers, perform the transaction or update the account.
2. Information that is presented to the customer has to be authentic reliable accurate
3. Internet banking software verify action to prevent accidental improper modification to the account, by the account holders or the supervisor (prevent improper modification by authorised users)
4. System ensure internal and external consistency - Account stats and receipts must be equal (needed for transactions)

Question 5

Explain what a security model is. How is a security model different from a security policy?

Security Model: Preventing escalation. Modeling task in user level and

Specifying data structures and techniques to ensure

Math

Enforce security policy

Security Policy: outline goals wo reg to how they are gg to be accomplished.

Particular situation

Security model

* Preventing privilege escalation and modeling users performing different task at the user level and the admin level
* Maps the abstract goal of the policy to information system terms by specifying explicit data structures and techniques necessary for the security policy
* Usually represented in Mathematics and identical ideas which are mapped to system modifications and then, developed by programmers through programming code
* Takes the requirements and provide the necessary mathematical formulas relationships and structures to be followed and to accomplish the goals. From there, the specifications are developed per operating system and the individual members can decide how they are going to implement these mechanisms that meet these necessary specifications
* Developed to enforce security policies

Security Policy

* Encompasses security goals such as each subject has to be authorised to access each object
* Outline the goals without regard to how they will be accomplished while a model is a framework that gives the policy for and solves security access problems for a particular situation

A security policy is a statement that outlines how entities access each other, what operations different entities can carry out, what level of protection is required for a system or software product, and what actions should be taken when these requirements are not met. The policy outlines the expectations that the hardware and software must meet to be considered in compliance. A security model outlines the requirements necessary to properly support and implement a certain security policy. If a security policy dictates that all users must be identified, authenticated, and authorized before accessing network resources, the security model might lay out an access control matrix that should be constructed so it fulfills the requirements of the security policy. If a security policy states that no one from a lower security level should be able to view or modify information at a higher security level, the supporting security model will outline the necessary logic and rules that need to be implemented to ensure that under no circumstances can a lower-level subject access a higher-level object in an unauthorized manner. A security model provides a deeper explanation of how a computer operating system should be developed to properly support a specific security policy.

Question 6 Describe a security model designed to provide integrity protection.

Biba Model

3 main rules:

1. No write up
2. No read down
3. Subject cannot request service to subjects of higher integrity

Question 7 Explain how the Bell-LaPadula model determines if a particular subject can access a requested object.

Bell-lapadula

How subj access object

* Works on subj clearance. Metrics and security level which is used to determine if subj can access different objects
* Subject clearance is then compared to the object classification and then specific rules are applied to control how subject to object interactions take place

Question 8

Consider the case in which you have been hired as a security expert by a large accounting corporation to advise on the most appropriate security model to be used in the corporation’s software. The options are the Bell-LaPadula model or the Biba model. Specify which model you would select and explain your reasoning.

Integrity goals:

Prevent unauthorised

Separation of duties: prevent improper modifications

Maintain consistency and reliability of information

* For this question, Accounting (achieve CIA !!) is the key
* However in this question, I is of higher priority
* For this type of question, identify where Confidentiality or Availability have higher priority

Eg.

* Commercial industry - Integrity of the data
* Accounting firm - tallying its numbers and making sure that decimal points are not dropped or whether there are extra zeros added in the process carried out by an application.

Ensure that there are well formed transactions

(Integrity of these data)

Under threat of people stealing these numbers

Use software that employs the Biba Model

Accounting firm - tallying its numbers and making sure that decimal points are not dropped or whether there are extra zeros added in the process carried out by an application.

* Ensure that there are well formed transactions
* (Integrity of these data)
* Under threat of people stealing these numbers
* Use software that employs the Biba Model

Question 9

Both the Clark-Wilson and Biba models address the issue of integrity. Given that integrity models have three major goals, specify the integrity goals and indicate the goals addressed by each model

Integrity models 3 main goals

* Information integrity—Is a given piece of information valid/correct?
* Data integrity—Has a given piece of information been modified?
* Origin integrity—Where did a piece of information come from?

Question 10

Suppose that the Clark-Wilson security model is used by a bank to implement an Internet banking system so that customers can access their accounts and perform transactions online using an Internet browser on a computer. From the customer’s perspective, give an example of the relevant part of the Internet banking system best describes.

* Constrained data items (CDIs)
* Unconstrained data items (UDIs)
* Transformation procedures (TPs)

For each example, briefly describe your reasoning.

\* Read slides to understand the different models then understand the banking example

CDIs

Example: Transaction data

because they need to be protected from improper modifications

UDI

Example: Personal information abt users which can be modified by the users

Do not need high level of protection, unlike the transaction data

TPs

Example: Client side banking software which performs authentication and communicates with the bank data base and server to ensure read or write requests are proper. It also converts CDIs to UDIs for the user to update

Integrity Verification Procedure

Server side (at the backend) that ensures high data consistency so that the transaction can be successfully completed and the increase in one account is exactly equal to the decrease of another account. Often, the user is notified that the transaction is successful due to the Integrity Verification Procedure

Extra knowledge:

A cyber security transformation enables you to rapidly reduce cyber risk and confidently adopt new digital technologies that support your strategic goals.

**Trends of different businesses in cyber security**

Attack Surface: Supply chain

Business Trend: The extended network is growing, increasing collaboration and joint ventures with business partners to develop digital-centric customer experiences.

Risk: More connections with external parties which can be exploited to steal data or disrupt customer services.

Attack Surface: Remote working

Business Trend: The workforce is evolving, with more users connected remotely than ever before, anywhere in the world and using any device.

Risk: Access and exfiltration of sensitive data due to poorly managed credentials and weak authentication mechanisms.

Attack Surface: Internet of things (IoT)

Business Trend: Organisations are modernising the way they work by adopting internet-enabled devices that can provide telemetry data to support and monitor specific business use cases.

Risk: Use of connected IoT devices increases both the proliferation of unmanaged sensitive data and vulnerability to large scale, multi-vector fifth generation cyber attacks.

Attack Surface: Digital channels

Business Trend: Innovation and redesign of traditional digital platforms are transforming the customer experience, improving the ability to reach new consumers and offer more services online.

Risk: More online touchpoints with customers and business partners serving increasingly rich and valuable data which can be targeted to steal or manipulate such data.

Attack Surface: Cloud

Business Trend: The organisation is accelerating its adoption of public cloud hosted services to improve agility and innovation.

Risk: Core business workload is increasingly hosted on cloud infrastructure which, if poorly configured, can be compromised to steal data or disrupt critical services.