### 

### **3413ICT Network Security**

### **Workshop – 12B**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Review Questions:**   1. Explain what a Trusted System is.   A system believed to enforce a given set of attributes to a stated degree of assurance.   1. What is TPM?   Trusted Platform Module  The TC approach employs a TPM chip in personal computer motherboard  or a smart card or integrated into the main processor, together with hardware and  software that in some sense has been approved or certified to work with the TPM.  We can briefly describe the TC approach as follows. The TPM generates keys that  it shares with vulnerable components that pass data around the system, such as  storage devices, memory components, and audio/visual hardware. The keys can be  used to encrypt the data that flow throughout the machine. The TPM also works  with TC-enabled software, including the OS and applications. The software can be  assured that the data it receives are trustworthy, and the system can be assured that  the software itself is trustworthy.    To achieve these features, TC provides three basic services: authenticated  boot, certification, and encryption.     1. Explain what cloud computing is. Describe the advantages of cloud computing.   Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.   1. List and discuss several priorities of cloud-computing service providers.  * Effectively meet the advertised services, while optimizing cloud resource utilization * Offer tenants capabilities for self-service * Ensure confidentiality, integrity, and availability, as well as security assurance in a multi-tenant environment  1. In addition to traditional data confidentiality, integrity, availability, and privacy, what other security concerns do cloud users have?  * The cloud acts as a big black box, nothing inside the cloud is visible to the clients * Clients have no idea or control over what happens inside a cloud * Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity  1. List and explain the common IT security management functions.   Determining organizational security objectives, strategies & policies  Determining organizational security requirements  Identifying and analyzing security threats to IT assets  Identifying and analyzing risks  Specifying appropriate safeguards  Monitoring the implementation and operation of safeguards  Developing and implement a security awareness program  Detecting and reacting to incidents   1. Explain the process of IT security management. Explain why IT security management is not something undertaken just once; rather it is a cyclic process that must be repeated.   IT SECURITY MANAGEMENT: A process used to achieve and maintain appropri- ate levels of confidentiality, integrity, availability, accountability, authenticity, and reli- ability. IT security management functions include:  • determining organizational IT security objectives, strategies, and policies  • determining organizational IT security requirements  • identifying and analyzing security threats to IT assets within the organization  • identifying and analyzing risks  • specifying appropriate safeguards  • monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization  • developing and implementing a security awareness program  • detecting and reacting to incidents  Rather it is a cyclic process that must be repeated constantly in order to keep pace with the rapid changes in both IT technology and the risk environment.   1. List and briefly explain the four approaches to identifying and mitigating IT risks.   **Baseline approach**: The goal is to implement agreed controls to provide protection against the most common threats    **Informal approach**: It conducts informal, pragmatic risk analysis on organization’s IT systems. A major advantage of this approach is that the individuals performing the analysis require no additional skills. These may either be internal experts if available, or alternatively external consultants  **Detailed risk analysis**:   * It uses formal structured process   + consists of a number of stages   + identifies threats and vulnerabilities to assets   + identifies likelihood of risk occurring and consequences   **Combined approach**:   * It combines elements of other approaches   + initial baseline on all systems   + informal analysis to identify critical risks   + formal assessment on these risks  1. A number of standards document the expected formal risk assessment approach. Explain the steps in the risk assessment approach.   **Establishing the context**: Its purpose is to determine the basic parameters within which the risk assessment will be conducted, and then to identify the assets to be examined.    **Asset identification**: An **asset is “anything that needs to be protected” because**  it has value to the organization and contributes to the successful attainment of  the organization’s objectives  **Threat Identification**: Anything that might hinder or prevent an asset from providing appropriate levels of the key security services    **Threat Sources**: Include damage caused by fire, flood, storm, earthquake, and other such natural events. It also includes environmental threats such as long term loss of power or natural gas. Or it may be the result of chemical contamination or leakage. Alternatively, a threat source may be a human agent acting either directly or indirectly.  **Analyse Risks**: The aim is to identify and categorize the risks to assets that threaten  the regular operations of the organization. Risk analysis also provides information  to management to help managers evaluate these risks and determine how best to  treat them.  **Analyse Existing Controls**: Before the likelihood of a threat can be specified,  any existing controls used by the organization to attempt to minimize threats need  to be identified   1. When evaluating possible human threat sources, what factors should be considered? Explain these factors.   • Motivation: Why would they target this organization; how motivated are they?    • Capability: What is their level of skill in exploiting the threat?   * Resources: How much time, money, and other resources could they deploy?     • Probability of attack: How likely and how often would your assets be targeted?    • Deterrence: What are the consequences to the attacker of being identified?     1. Given the probability that threat occurs and the consequence to the organization (or called cost to organization), what is the simple equation for determining risk?   Risk = (Probability that threat occurs) \* (Cost to organization)   1. What are the items specified in the risk register for each asset or threat identified?  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Asset** | **Threat/ Vulnerability** | **Existing Controls** | **Likelihood** | **Consequence** | **Level of Risk** | **Risk Priority** |  * **Risk acceptance** * **Risk avoidance** * **Risk transfer** * **Reduce consequence** * **Reduce likelihood**  1. List and explain the five alternatives for treating identified risks.   **Risk acceptance**: Choosing to accept a risk level greater than normal for busi- ness reasons. This is typically due to excessive cost or time needed to treat the risk. Management must then accept responsibility for the consequences to the organization should the risk eventuate.  **Risk avoidance**: Not proceeding with the activity or system that creates this risk. This usually results in loss of convenience or ability to perform some function that is useful to the organization. The loss of this capability is traded off against the reduced risk profile.  **Risk transfer**: Sharing responsibility for the risk with a third party. This is typically achieved by taking out insurance against the risk occurring, by enter- ing into a contract with another organization, or by using partnership or joint venture structures to share the risks and costs should the threat eventuate  **Reduce consequence**: By modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur. This could be achieved by implementing controls to enable the organization to quickly recover should the risk occur. Examples include implementing an off-site backup process, developing a disaster recovery plan, or arranging for data and processing to be replicated over multiple sites.  **Reduce likelihood**: By implementing suitable controls to lower the chance of the vulnerability being exploited. These could include technical or administra- tive controls such as deploying firewalls and access tokens, or procedures such as password complexity and change policies. Such controls aim to improve the security of the asset, making it harder for an attack to succeed by reducing the vulnerability of the asset. |