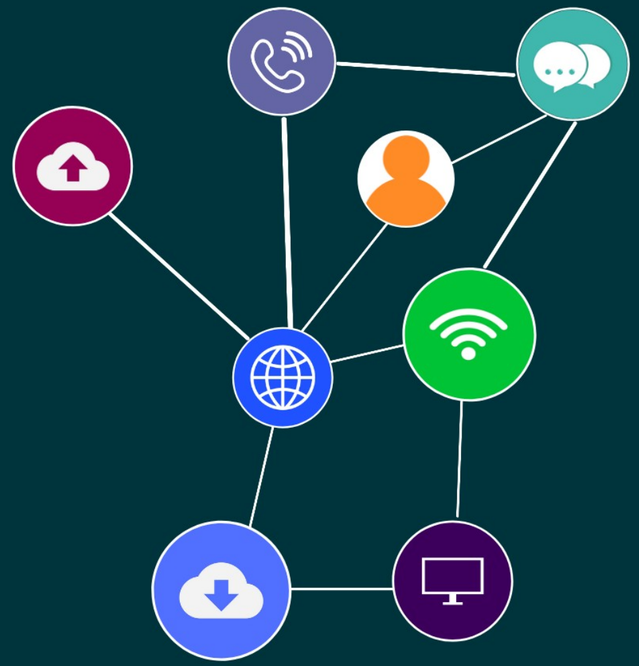
ICTNWK546

Manage network security



MILESTONES
International College

Topic 1: Plan security design process

PLANNING PHASE FOR NETWORK SECURITY DESIGN

- Taking on a project for managing network security can be a complex task. Project management can be key to a successful ICT project.
- The methodologies used in project management are a series of different processes designed to assist project managers and those overseeing or involved with projects.

Topic 1: Plan security design process

ICT NETWORKS

When defining the planning phase for a security design, it is important to understand different ICT networks and their configuration as their differences can affect the way in which the design can be implemented.

Topic 1: Plan security design process

ACTIVITY: RESEARCH AND DISCUSS

Using the following links, describe three networks and their configurations.

Common network topologies:

http://www.firewall.cx/networking-topics/general-networking/103-network-topologies.html

https://en.m.wikibooks.org/wiki/Communication_Networks/Network_Topologies

The trainer/assessor will facilitate a class discussion about the outcomes from the research.

Topic 1: Plan security design process

ACTIVITY: READ

The listed articles provide an overview of wireless topologies.

Topic 1: Plan security design process

PLANNING FOR NETWORK SECURITY DESIGN

The planning phase is the most important aspect of any project. It will define the way in which the project will be undertaken and be used as a framework for the other stages of the project.

Topic 1: Plan security design process

ACTIVITY: PRACTICAL

Using the RTO network, or one that you have access to, review the network infrastructure.

List down as much information as you can about the network.

Draw a network diagram of the current system.

Topic 1: Plan security design process

BUILDING PHASE FOR NETWORK SECURITY DESIGN

In the building phase, network administrators and security specialists use the available hardware and software to create the security system as set out in the security design.

MANAGING PHASE FOR NETWORK SECURITY DESIGN

After the security design has been implemented, the administrator is responsible for managing the design to ensure it provides the security envisioned by the security design.

ORGANISATIONAL REQUIREMENTS

- You always need to ensure your activities align with organisational requirements relating to the planning, building and managing phases.
- These can be identified by talking with senior management and co-workers, reading internal policies and procedures and observing what others do ion the workplace.

Topic 2: Identifying threats to network security

DETERMINING WHY ATTACKS OCCUR

To identify threats to the network security you have to determine why the attacks are occurring.

Network attacks can be:

Passive		Active
Where an attacker will just gain access to a network.		Where an attacker will gain access to a network and modify, delete, steel, harm or encrypt data.

Topic 2: Identifying threats to network security

DETERMINING WHO THE ATTACK MAY COME FROM

To determine who the attack may come from, you need to ensure that the network uses different mechanisms to successfully identify and classify the threats or attacks. You can use specific techniques to identify and classify these.

COMMON TYPES OF NETWORK VULNERABILITIES

- poor configurations
- inaccurate authorisations
- interception
- privilege escalation
- internal threats
- external threats and viruses
- social engineering.

Topic 2: Identifying threats to network security

DETERMINING HOW ATTACKS OCCUR

Some common attacks are:

- Dos (Denial of Service) Attack
- Modification of Data
- IP address spoofing
- Man in the middle attack
- Phishing

Topic 2: Identifying threats to network security

SECURITY TECHNOLOGIES

Using security technologies can support dealing with the threat of attacks and network vulnerabilities.

Network security technologies cover both hardware and software threats.

Topic 2: Identifying threats to network security

EMERGING SECURITY ISSUES

With the expansion of cloud services and new technologies, the use of mobile devices and the Internet of Things (IoT), there have also emerged a number of security issues.

THREAT MODELS USED TO CATEGORISE THREATS

Threat modelling is used as a systematic and structured approach used to understand an environment and identify vulnerabilities and potential attacks and identify how to mitigate them.

ACTIVITY: READ

Threat models explained:

https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html

Take any notes to summarise what you have read and keep for future reference.

Topic 2: Identifying threats to network security

ACTIVITY: RESEARCH AND REPORT

Divide into small groups.

You are to research one network system. This could be at the RTO where you are studying, approved by the trainer/assessor or your place of work.

Topic 2: Identifying threats to network security

Topic 3: Analysing security risks

ELEMENTS OF RISK MANAGEMENT

- A security strategy outlines major security concerns and the way in which an organisation will deal with them.
- Risk management is a process used to identify, assess and control threats.

ACTIVITY: READ

Read more on the elements of the risk management process:

https://www.corporatecomplianceinsights.com/key-elements-of-the-risk-management-process/

Take any notes to summarise what you have read and keep for future reference.

Topic 3: Analysing security risks

ELEMENTS OF RISK MANAGEMENT

Risk management can help to protect an organisation’s assets, prevent data loss, theft or corruption, manage system or application failure or downtime, meet compliance requirements and from internal and external security threats.

ASSETS REQUIRING PROTECTION

The next step to analysing security risks is to determine the assets that require the most protection.

Assets can include:

- data and information
- hardware and software.

ACTIVITY: GROUP WORK

Divide into small groups. Ensure you divide the work equally.

Create a spreadsheet to record assets for hardware in the room allocated by the trainer/assessor.

List each asset with a brief description of each.

What further assets would require protection and why?

Topic 3: Analysing security risks

CATEGORISING ASSETS AND CALCULATING THEIR VALUE

It is then necessary to define standards for determining the importance of each asset. A list of criteria can be used so that you can prioritise each one through classification.

ACTIVITY: READ

How to conduct an IT asset evaluation:

https://www.exittechnologies.com/blog/it-tips/the-it-asset-valuation-guide/

Take any notes to summarise what you have read and keep for future reference.

Topic 3: Analysing security risks

ACTIVITY: GROUP WORK

Divide into your previous groups. Ensure you divide the work equally.

Refer back to the spreadsheet you created to record assets for hardware.

For each asset listed, work out a way in which you can categorise these.

Work out a value for each asset.

Using a relevant function on the spreadsheet, sort the data so that you can clearly see the assets that hold the most priority and biggest risk if they were to be lost, stolen, damaged or corrupted.

RISK MANAGEMENT PLANS

- A risk management plan can be used to minimise any impacts of potential risk by using a strategy to deal with them.
- Having a risk management plan and procedures is vital for network security.

ACTIVITY: READ

An example of a risk management plan:

https://www.northam.wa.gov.au/documents/708/sample-risk-management-plan

Source a risk management plan that relates to ICT.

Develop a risk management plan that could be used for the network allocated to you by the trainer/assessor. You must include the risk of data loss, corruption, theft, and privacy and confidentiality of student information. Address both internal and external threats.

Topic 3: Analysing security risks

ORGANISATIONAL REQUIREMENTS

Standard practice is that all risk management activities when implementing and managing security functions throughout a network must align and comply with organisational risk management requirements.

Topic 4: Create a security design

ATTACKER SCENARIOS AND THREATS

The use of attacker scenarios and threats can be used to simulate or predict the types of attack that may occur and thus put in measures to help prevent them.

ACTIVITY: READ

Read through the following attack scenario for virtual machine runtime hack:

https://www.sciencedirect.com/topics/computer-science/attack-scenario

Classifying network attack scenarios using an ontology approach:

https://core.ac.uk/download/pdf/145042558.pdf

Take any notes to summarise what you have read and keep for future reference.

Topic 4: Create a security design

SECURITY MEASURES FOR NETWORK COMPONENTS

There are specific measures that you can take for securing network components e.g. auditing and penetration testing techniques can be used to measure a network's security.

NETWORK CONTROLS

Network controls use solutions to control access into and out of a network. These are usually outlined in the security policies and procedures; and risk management plan.

NETWORK ACCESS CONTROL (NAC)

This is a security measure, using a set of protocols to define and implement a policy, that describes how to secure access to network nodes by devices when they attempt access.

DEVELOPING SECURITY POLICIES

- Security policies provide a set of guidelines and rules to follow for computer network access.
- It is a formal document communicated at management level, outlining the principles, procedure and guidelines to enforce, manage and protect a company’s network.

SUBMISSION OF DOCUMENTATION

When all the above documents (such as policies, plans, protocols) have been prepared you need to provide these to ‘relevant persons’ and request their comment by a set date.

ACTIVITY: READ

Review the following network security policy for the Villanova University:

https://www1.villanova.edu/villanova/unit/policies/AcceptableUse/security.html

An example of a security policy - Network protection and information security policy:

https://txwes.edu/media/twu/content-assets/documents/it/Network-Protection-and-Info-Security-Policy.pdf

Topic 4: Create a security design

ACTIVITY: GROUP WORK

Divide into small groups. Ensure you divide the work equally.

Research a network security policy that could be used in an educational context in Australia.

Use the policy as a guidance to create an outline for a network security policy for the network allocated by the trainer/assessor for this task. Add suitable control methods that can be used as well any countermeasures.

Topic 4: Create a security design

Topic 5: Design security incidents response

AUDITING AND INCIDENT RESPONSE PROCEDURES

An incident response procedure is a method used for handling security breaches, threats and incidences. It can help to identify and effectively minimise damages or costs caused by the incident as well as finding and fixing the cause.

Topic 5: Design security incidents response

ACTIVITY: READ

Cyber Security Incident Response guide:

https://justinweeks.keybase.pub/Infosec/CSIR-Procurement-Guide.pdf?dl=1

Take any notes to summarise what you have read and keep for future reference.

Topic 5: Design security incidents response

AUDITING AND INCIDENT RESPONSE PROCEDURES

- Audits can be undertaken to identify any risks of a security breach, as well as determining the effectiveness of the preventative measures.
- An audit can include a review of both physical and logical measures.

Topic 5: Design security incidents response

DOCUMENTING SECURITY INCIDENTS

- All security incidents should be clearly and sufficiently documented.
- This ensures that there is an audit trail and also can be used as future reference for any further incidents

Topic 5: Design security incidents response

IMPLEMENTING CONFIGURATIONS FROM INCIDENT RESPONSE PROCEDURES

An incident response outcome can be used to analyse and plan solutions to any compromised networks. It could include implementation of new configurations to countermeasure an attack.

Topic 5: Design security incidents response

TESTING

Perhaps the second most important part of managing network security (other than planning) would be testing phase. Testing should be carried out on a continual basis during the analysis, design and implementation of the network security design.

Topic 5: Design security incidents response

ACTIVITY: READ

Network security testing:

https://www.secureworks.com/centers/network-security

Penetration testing:

https://www.imperva.com/learn/application-security/penetration-testing/

Take any notes to summarise what you have read and keep for future reference.

Topic 5: Design security incidents response

SUBMISSION FOR SIGN OFF

- You need to provide all completed documents to the client for their final approval as a distinct stage in the overall process.
- Obtaining sign-off for the network security design could be from a supervisor, client or any relevant stakeholders.

Topic 5: Design security incidents response