UNIVERSITI TEKNIKAL MALAYSIA MELAKA

PEPERIKSAAN PERTENGAHAN SEMESTER I
MID SEMESTER EXAMINATION SEMESTER I
SESI 2021/2022
SESSION 2021/2022

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD MATAPELAJARAN ***SUBJECT CODE***	**:**	**BITS 3363**
MATAPELAJARAN ***SUBJECT***	**:**	**KESELAMATAN RANGKAIAN PENGURUSAN PROJEK** ***NETWORK SECURITY PROJECT MANAGEMENT***
PENYELARAS ***COORDINATOR***	**:**	**DR. ZAHEERA BINTI ZAINAL ABIDIN**
KURSUS ***COURSE***	**:**	**BITZ**
MASA ***TIME***	**:**	**4:00 – 6:00 petang** ***4:00 – 6:00 p.m.***
TEMPOH ***DURATION***	**:**	**2 JAM** ***2 HOURS***
TARIKH ***DATE***	**:**	**15 NOVEMBER 2021** ***15 NOVEMBER 2021***
TEMPAT ***VENUE***	**:**	

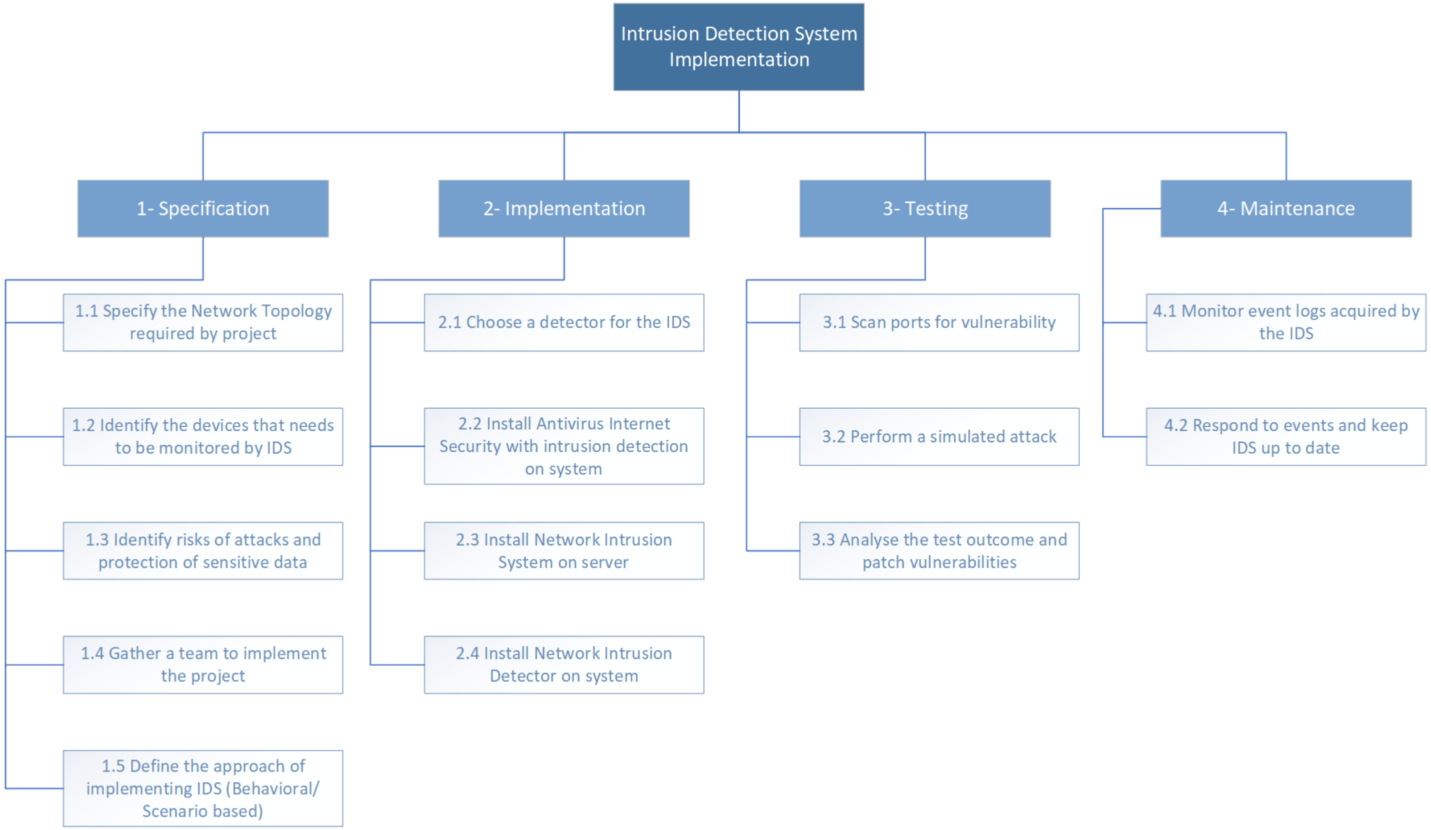
NAMA PELAJAR ***STUDENT NAME***	**: Muhammad Izham Bin Norhamadi**
NOMBOR MATRIK PELAJAR ***STUDENT MATRIC NUMBER***	**: B032020039**

QUESTION 1 (25 MARKS)

As a project manager, you need to set up an Intrusion Detection System (IDS) for your client at the main server room. The purpose of IDS is to filter packets either in-going or out-going or both ways of the network traffic.

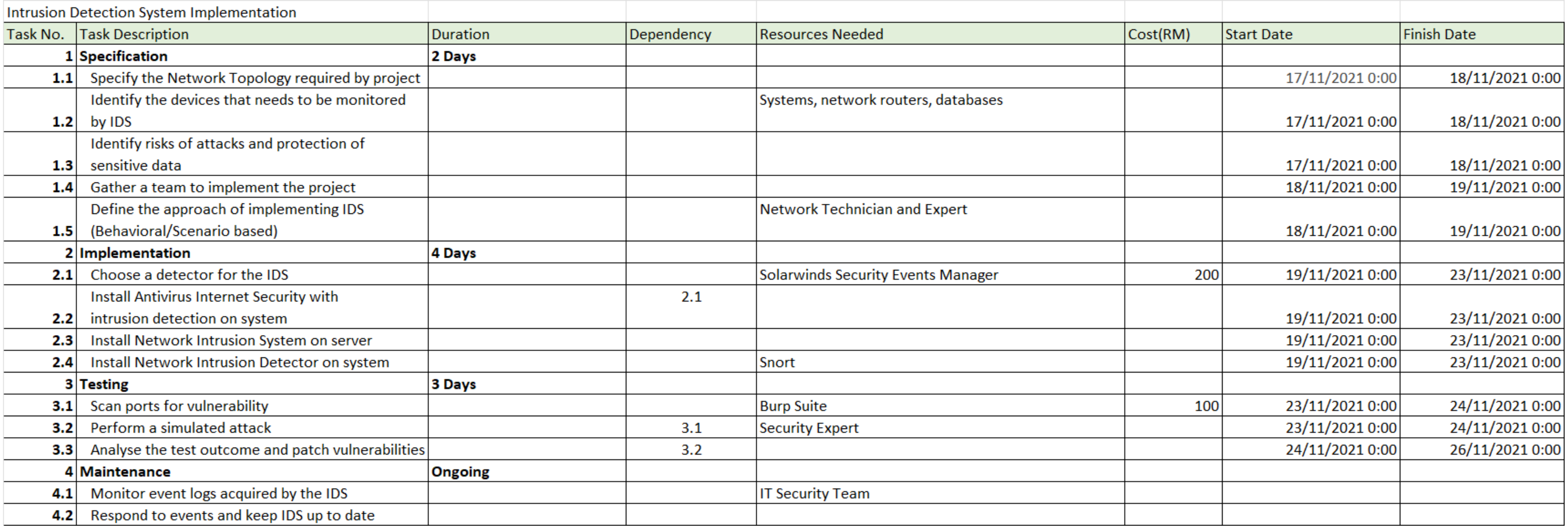
a. Draw a diagram of Work Breakdown Structure (WBS) for IDS implementation.

(6 Marks)


Intrusion Detection System Implementation
1- Specification
2- Implementation
3- Testing
4- Maintenance
1.1 Specify the Network Topology required by project
1.2 Identify the devices that needs to be monitored by IDS
1.3 Identify risks of attacks and protection of sensitive data
1.4 Gather a team to implement the project
1.5 Define the approach of implementing IDS (Behavioral/ Scenario based)
2.1 Choose a detector for the IDS
2.2 Install Antivirus Internet Security with intrusion detection on system
2.3 Install Network Intrusion System on server
2.4 Install Network Intrusion Detector on system
3.1 Scan ports for vulnerability
3.2 Perform a simulated attack
3.3 Analyse the test outcome and patch vulnerabilities
4.1 Monitor event logs acquired by the IDS
4.2 Respond to events and keep IDS up to date

b. Demonstrate the WBS Dictionary from one of the WBS created as mentioned in 1(a).

(6 Marks)



Intrusion Detection System Implementation

Task No.	Task Description	Duration	Dependency	Resources Needed	Cost(RM)	Start Date	Finish Date
1	**Specification**	**2 Days**					
1.1	Specify the Network Topology required by project					17/11/2021 0:00	18/11/2021 0:00
1.2	Identify the devices that needs to be monitored by IDS			Systems, network routers, databases		17/11/2021 0:00	18/11/2021 0:00
1.3	Identify risks of attacks and protection of sensitive data					17/11/2021 0:00	18/11/2021 0:00
1.4	Gather a team to implement the project					18/11/2021 0:00	19/11/2021 0:00
1.5	Define the approach of implementing IDS (Behavioral/Scenario based)			Network Technician and Expert		18/11/2021 0:00	19/11/2021 0:00
2	**Implementation**	**4 Days**					
2.1	Choose a detector for the IDS			Solarwinds Security Events Manager	200	19/11/2021 0:00	23/11/2021 0:00
2.2	Install Antivirus Internet Security with intrusion detection on system		2.1			19/11/2021 0:00	23/11/2021 0:00
2.3	Install Network Intrusion System on server					19/11/2021 0:00	23/11/2021 0:00
2.4	Install Network Intrusion Detector on system			Snort		19/11/2021 0:00	23/11/2021 0:00
3	**Testing**	**3 Days**					
3.1	Scan ports for vulnerability			Burp Suite	100	23/11/2021 0:00	24/11/2021 0:00
3.2	Perform a simulated attack		3.1	Security Expert		23/11/2021 0:00	24/11/2021 0:00
3.3	Analyse the test outcome and patch vulnerabilities		3.2			24/11/2021 0:00	26/11/2021 0:00
4	**Maintenance**	**Ongoing**					
4.1	Monitor event logs acquired by the IDS			IT Security Team			
4.2	Respond to events and keep IDS up to date						

c. Work is organized in WBS according to its estimated duration, cost, talent, and resource requirements. What is the work element?

(2 Marks)

- The smallest unit of work that can be performed independently

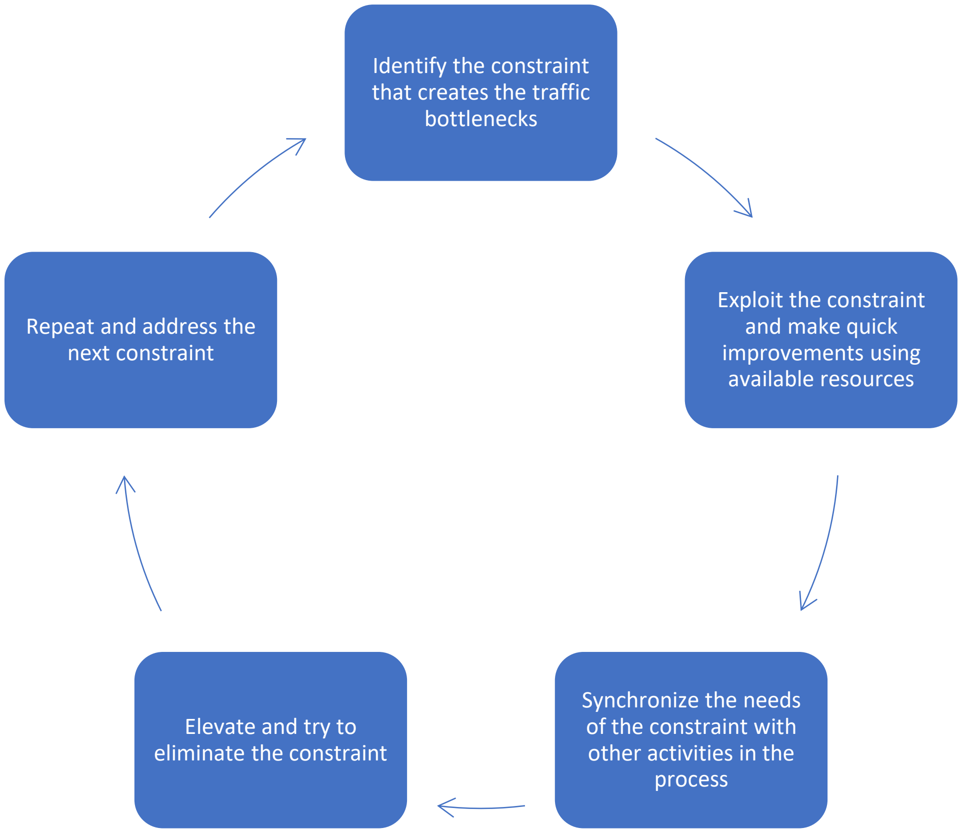
d. Explain **THREE (3)** ways to shorten a project schedule during the IDS implementation.

(6 Mark)

1. Shorten lag time between tasks
   If tasks on the critical path include lag time between them, reducing that lag time is an easy way to shorten the project duration. In IDS implementation, installing Network Intrusion System and Network Intrusion Detector simultaneously can reduce the lag time in critical path.
2. Establish the scope of the project
   Establishing scope of the IDS before the project team is assembled reduces the non-productive time at the beginning of the project. Make sure thoroughly analyse valuable assets in organization that needs to be monitored.
3. Fast-tracking project
   Tasks in critical path that can be conducted in parallel can shorten the schedule without increasing the cost. In IDS planning, we can specify the network topology that is required and identifying the devices that needs to be monitored at the same time.

e. You have halfway through testing the IDS servers. However, you are experiencing traffic bottlenecks, which delay the progress of the project. You need to get back on track and the theory of constraints is one of the techniques to solve the problem. Investigate the constraint that creates bottlenecks at the IDS server.

(5 Marks)


Identify the constraint that creates the traffic bottlenecks
Exploit the constraint and make quick improvements using available resources
Synchronize the needs of the constraint with other activities in the process
Elevate and try to eliminate the constraint
Repeat and address the next constraint

QUESTION 2 (25 MARKS)

As a network security project manager, you are responsible to ensure the quality of network security services and prevent mistakes occurred in the organization.

a. List **TWO (2)** mistakes that commonly happen in the network environment.

(2 Marks)

1. High bandwidth usage
2. Network misconfiguration

b. Define **THREE (3)** types of network security testing used in preventing malware in the network environment.

(6 Marks)

1. Vulnerability Scanning – A vulnerability scan that makes use of an automated tool to scan systems and networks for known vulnerabilities and give you a list of detected security flaws.
2. Penetration Testing – Also known as ethical hacking is described as intentional launching of simulated cyberattacks to identify exploitable issues on systems and networks using testing techniques and testing tools.
3. Traffic monitoring – A method of monitoring incoming and outgoing traffic on a computer network via specialized hardware or software such as Wireshark in real time to find any anomalies.

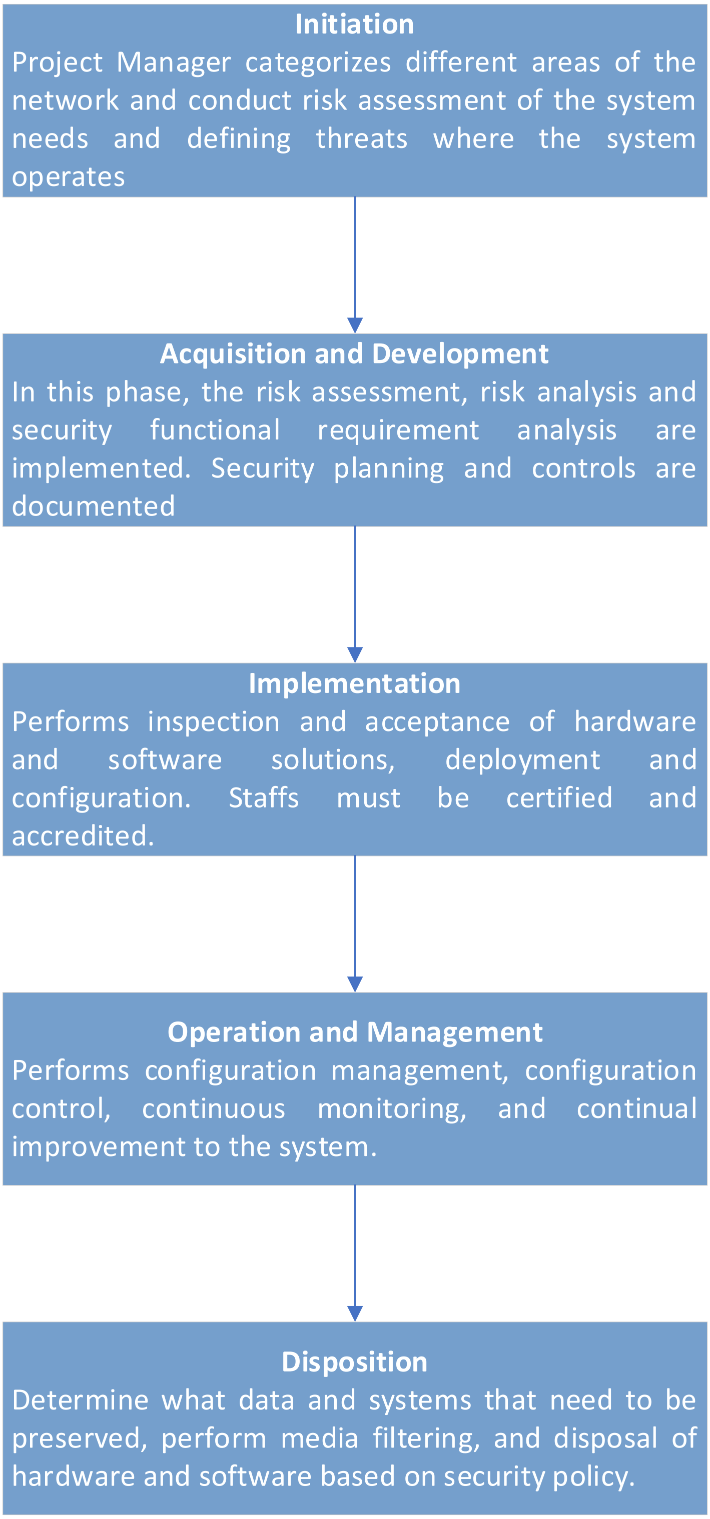
c. Explain **THREE (3)** strategies for preventing human mistakes at the company.

(6 Marks)

1. Offer and invest in staff training – Training and training tools directly address employee knowledge and experience. A thorough training can help bridges any knowledge or experiential gaps employees may have, and it ensures employees are on the same page.
2. Create and maintain an effective communication line – By making sure that communications are clear and concise, we can prevent errors occurring from miscommunications. Bolster a stronger communication line between staff will make briefs, project management and evaluations a much more streamline process where everyone is on the same page.
3. Review safety and security practices often – Review tools used, update training modules, and change policies to adapt to requirements can reduce human error in workplace. Gather relevant information about your business to keep staff, tools and practices up to date reduce many instances of human error.

d. The root cause elements for network failure consist of People, Process, Technology, Controls, Procedure, and Environment. Demonstrate solution using FLOWCHART diagram from several root cause elements in increasing the quality of the system.

(5 Marks)



Initiation

Project Manager categorizes different areas of the network and conduct risk assessment of the system needs and defining threats where the system operates

Acquisition and Development

In this phase, the risk assessment, risk analysis and security functional requirement analysis are implemented. Security planning and controls are documented

Implementation

Performs inspection and acceptance of hardware and software solutions, deployment and configuration. Staffs must be certified and accredited.

Operation and Management

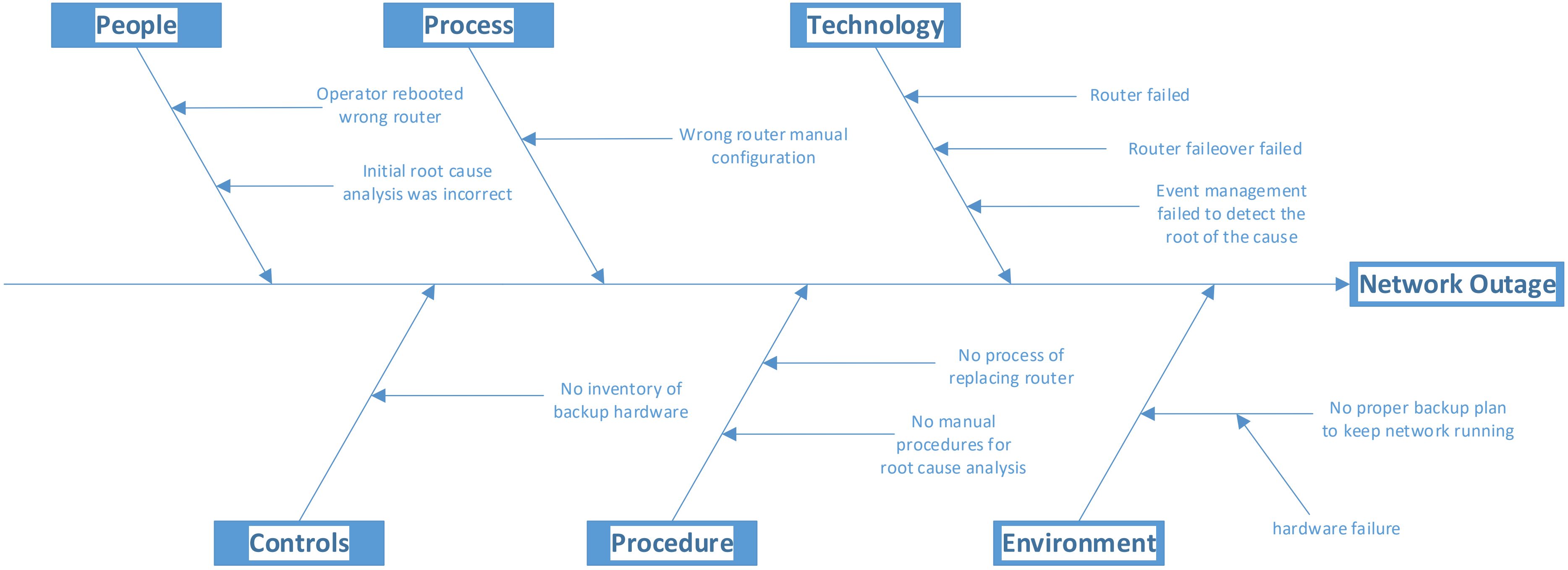
Performs configuration management, configuration control, continuous monitoring, and continual improvement to the system.

Disposition

Determine what data and systems that need to be preserved, perform media filtering, and disposal of hardware and software based on security policy.

e. A data centre had a serious network outage due to failed network router. The catastrophe has produced a total of four hours of network failures before the problem has been resolved. In a time of network failures, the security is easily breached by cyber attackers. Investigate the cause and effect to control the quality of network security performance using FISHBONE diagram.

(6 Marks)


People
Process
Technology
Operator rebooted wrong router
Initial root cause analysis was incorrect
Wrong router manual configuration
Router failed
Router faileover failed
Event management failed to detect the root of the cause
Network Outage
No inventory of backup hardware
No process of replacing router
No manual procedures for root cause analysis
No proper backup plan to keep network running
hardware failure
Controls
Procedure
Environment

QUESTION 3 (25 MARKS)

As a network security project manager, you are responsible for installing a new access control system in ABC Enterprise. You have identified problems that cause a negative outcome in the installation. Therefore, you are developing the risk management plan.

a. The newly installed access control system stores user profiles and demographic information on the cloud. However, you are concern about the data security and privacy during information transmission via cloud. Hence, you want to reduce the risk of cyber-attacks during the data communication. Explain **FIVE (5)** risk mitigations to reduce the risk and ensure data security.

(10 Marks)

1. Perform a risk assessment
   Risk assessments involve measures, processes, and controls to uncover potential gaps in organization security controls. A risk assessment can offer insight into assets that need to be protected and the security controls currently in place.
2. Create of patch management schedule
   Many software providers release patches consistently, which can be taken advantage of by cybercriminals to exploit a patch as soon as it was released. Thus, an organization should be aware of patch release schedule among their service and software providers to create an effective patch management schedule that can help security team stay ahead of attackers.
3. Continuous monitor of network traffic
   Some security tools provide real-time detection and cybersecurity mitigation that can help you gain a comprehensive view of your IT ecosystem at any point in time. This will allow IT security team to actively identify new threats and determine optimal path for remediation.

4. Prepare an incident response plan

   Ensuring that everyone, including both the IT security team and non-technical employees, knows what they're responsible for in the event of a data breach or attack can make it easier to have resources in place and ready to go. An incident response plan helps your organization do as much as possible to remain proactively prepared so your team can move quickly and efficiently to remediate any issues

5. Implement firewall and antivirus software

   Security solutions such as firewalls and antivirus software play an important role in cybersecurity risk mitigation strategy. Firewalls act as a buffer between the outside world and your network and gives your organization greater control over incoming and outgoing traffic. Similarly, antivirus software searches your device and network to identify any potentially malicious threats

b. Describe **FIVE (5)** approach to effectively communicate with the stakeholders to increase awareness on cyber-crimes and continuously gain support from the stakeholders.

(10 Marks)

1. Develop an Effective Security Strategy

   Built security into the culture of your organisation to ensure staff within the company understands the importance of cyber security and the impact of a data breach can have. Development of comprehensive security strategy will protect sensitive data, reduce threats and ensure the reputation of an organisation remains intact.

2. Get management invested in security

   Engaging with senior management and influential staff will add weight to any cyber security awareness program. Their involvement will show the high priority accorded to the initiative and how crucial security is. Top-down support will ensure those ultimately responsible for cybersecurity will help it succeed.

3. Conduct regular Cybersecurity Training

   Effective security awareness training is essential in training staff on how to identify and respond appropriately to growing range of cyber security threats. Cyber security training should be engaging and informative to ensure that staff understand what is required of them and their role in safeguarding sensitive data.

4. Keep Defensive Practices up to date

   Maintain security policies by having a thorough and continual way of monitoring cyber security compliance. It is vital for staffs to be continuously trained to ensure they can respond appropriately to the most up to date security threats.
5. Implement Cybersecurity drills

   Executing cybersecurity drills will allow the staff to learn and recognize various cyber attack scenarios that will help them prepared for the real threats such as email phishing.

c. Define **FIVE (5)** types of network security testing used in preventing malware in the network environment.

(5 Marks)

1. Vulnerability Scanning – A vulnerability scan that makes use of an automated tool to scan systems and networks for known vulnerabilities and give you a list of detected security flaws.
2. Penetration Testing – Also known as ethical hacking is described as intentional launching of simulated cyberattacks to identify exploitable issues on systems and networks using testing techniques and testing tools.
3. Traffic monitoring – A method of monitoring incoming and outgoing traffic on a computer network via specialized hardware or software such as Wireshark in real time to find any anomalies.
4. Conduct Audit and Risk Assessment – Identify the assets, talents, vulnerabilities, and potential threat to improve the Security Policy and Procedures.
5. Security Posture Assessment

QUESTION 4 (25 MARKS)

You are assigned to a large and complex project, which utilizes all project integration management processes and best practices. You have completed all activities associated with project initiation and have yet to begin project integration planning. You are preparing the project business documents, stakeholder register, and the sponsor has approved the project charter.

a. Discuss about the payback analysis of the project either the periodic cash inflows from the project is even or uneven.

(10 Marks)

Payback period is the time in which the initial outlay of an investment is expected to be recovered through the cash inflows generated by the investment. It is one of the simplest investment appraisal techniques. Payback period is an indicator of risk inherent in a project because it takes initial inflows into account and ignores the cash flows after the point at which the initial investment is recovered. Even cash flow refers to those cash flow in which the amount of each cash flow is same or equal at each period. Since this is a large and complex project, it would be likely to expect an even cash inflow for the project to generate in order to justify its initial investment. The payback period calculation is: Payback Period = Initial Investment/Net Cash Flow per Period. The longer the payback period of a project, the higher the risk, and the longer it takes to generate a profit. Project with high cash flow and short payback period is far more attractive to investors.

b. Compare the decision made by the network security project manager on even or uneven cash inflows.

(10 Marks)

Even Cash Inflow	**Uneven Cash Inflow**
Project Manager can capitalize on even amount cash flow to promote company's growth	Project Manager must be more careful in expanding the project as it can easily increase the payback risk

Project Manager can analyse quickly whether a project will generate a worthwhile income	Project Manager must plan for any increase or decrease in cash flow
Expected payback period are trustworthy, making the screening process for passing a project faster.	Project Manager must make be more detailed in calculating payback, as cash may flow equal or exceed the initial investment and requires a partial payback calculated.
Project Manager can attract investors to the project if the expected income is large to cover the initial cost	Project Manager must take care to not take too many investors to avoid being unable to fulfil debt
Requires minimal cash monitoring but instead focusing on regulating the project's cost	Project Manager is required to monitor the cash flow regularly

c. The monitoring project work progress produce corrective recommendation and prevention actions. Discuss about the performance of the project based on the corrective recommendation and preventive actions in securing the resources (such as confidential information, physical assets, data privacy and copyrighted ideas) in the organization.

(5 Marks)

- In a project management setting, Corrective action is the activity of reacting to a process problem, getting it under control through containment actions, and then taking the action needed to stop it from happening again while Preventive action is taken to fix the cause of a process problem before it can happen.

Corrective	**Preventive**
Analyse the amount of compromised data and make changes to the system to patch out the vulnerability	Prevent unauthorized access to sensitive information by securing it behind authentication and encryption

Analyse the damage to the assets, calculate the cost to recover the assets and invests in more security	Monitor valuable assets with surveillance camera and limit personnel access to the assets
Release a statement to company’s staff to change their password, and implement a new encryption to the private	Provide a strong encryption to staff’s private data
File a lawsuit in federal court for any copyright infringement of company’s properties	Enforce company’s copyrighted properties and clearly states what belongs to the company

-END OF QUESTIONS-