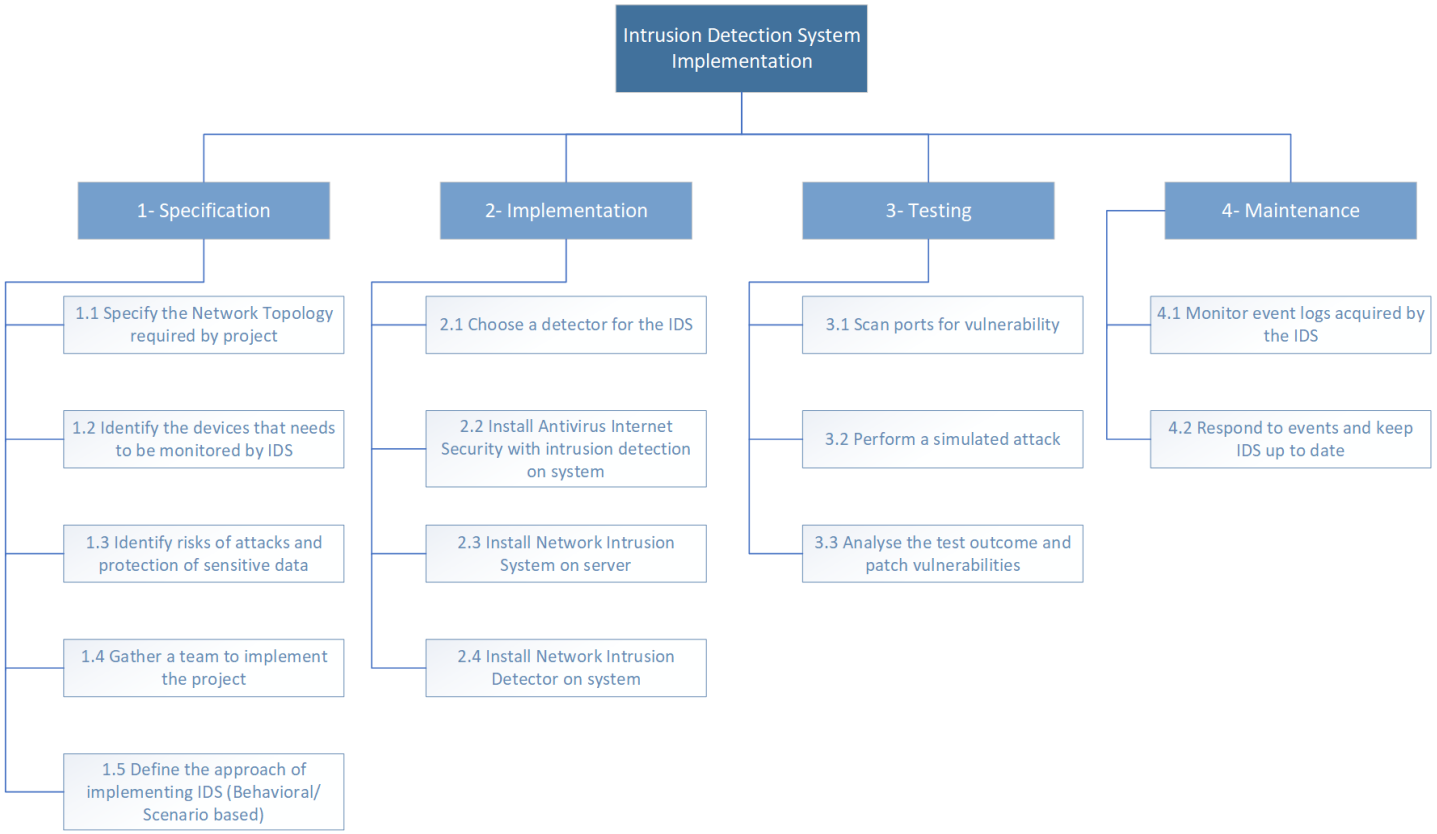
Muhammad Izham Bin Norhamadi
B032020039

FINAL EXAM BITS 3363

Question 1

a.



Muhammad Izham Bin Norhamadi
B032020039

b.

Specification

- The specification phase is where the project terms and requirements laid out by identifying the critical systems and networks that needs the monitoring service of IDS and the list of possible attacks that will be faced by the systems
- The duration of this phase takes 2 days
- The resources needed for this phase are system plans, network routers, and databases

Implementation

- The implementation phase is where the IDS will be implemented following the specifications of the project. A system was also selected to house the IDS and to secure the system and logs collected from tampering acts
- The duration of this phase takes 4 days
- The tools needed for this phase are SolarWinds Security Events Manager and Snort

Testing

- The testing phase will test and rate the security of the network by scanning for possible vulnerabilities and performing simulated attack. Identified vulnerabilities are patched and tested again
- The duration of this phase takes 3 days
- The resources needed for this phase are Security Experts and vulnerability scanning tools such as Burp Suite

Maintenance

- In this phase, a selected team of IT Security and Responders is required to monitor the logs on IDS for any unusual behaviour on the network and be prepared to respond to security events
- This is an ongoing phase until the phase returns to specification phase
- IT Security Team is required to maintain the IDS and responds to detections

c.

The smallest unit of work that can be performed independently

Muhammad Izham Bin Norhamadi
B032020039

d.

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

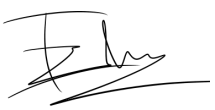
Establishing scope of the IDS before the project team is assembled reduces the non-productive time at the beginning of the project. Make sure to thoroughly analyse valuable assets in organization that needs to be monitored.

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.

It is important to swiftly rectify bottlenecks as they can restrict the flow of information, web applications, services, and employee workflow. In this scenario, the IDS deploys its detector on the Ethernet card, allowing the software to read and analyse all traffic. IDSs work in the same way as packet sniffers, looking for certain types of network attacks like packet floods and IP spoofing. The disc drive can become slow, which is a frequent bottleneck in systems which produces a lot of logs. A moderately fast CPU and main memory should not be performance obstacles if packets are just being written to disc for later analysis. If the memory is not enough for all the services, a possible solution is to use a bigger amount of the RAM for buffers.



Muhammad Izham Bin Norhamadi
B032020039

Question 2

a.

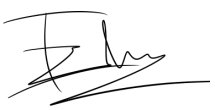
1. High bandwidth usage
2. Network misconfiguration

b.

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.

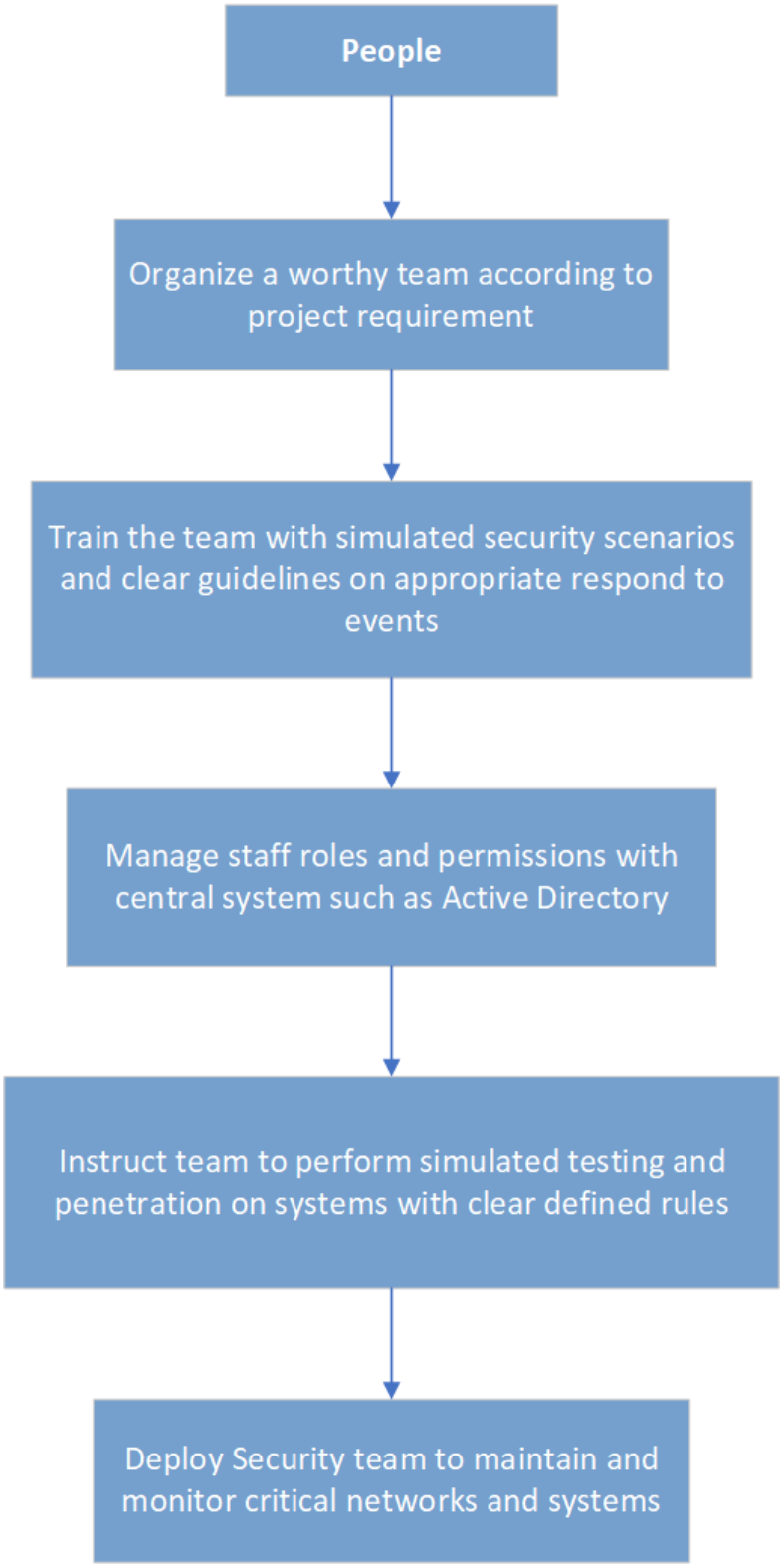
c.

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.



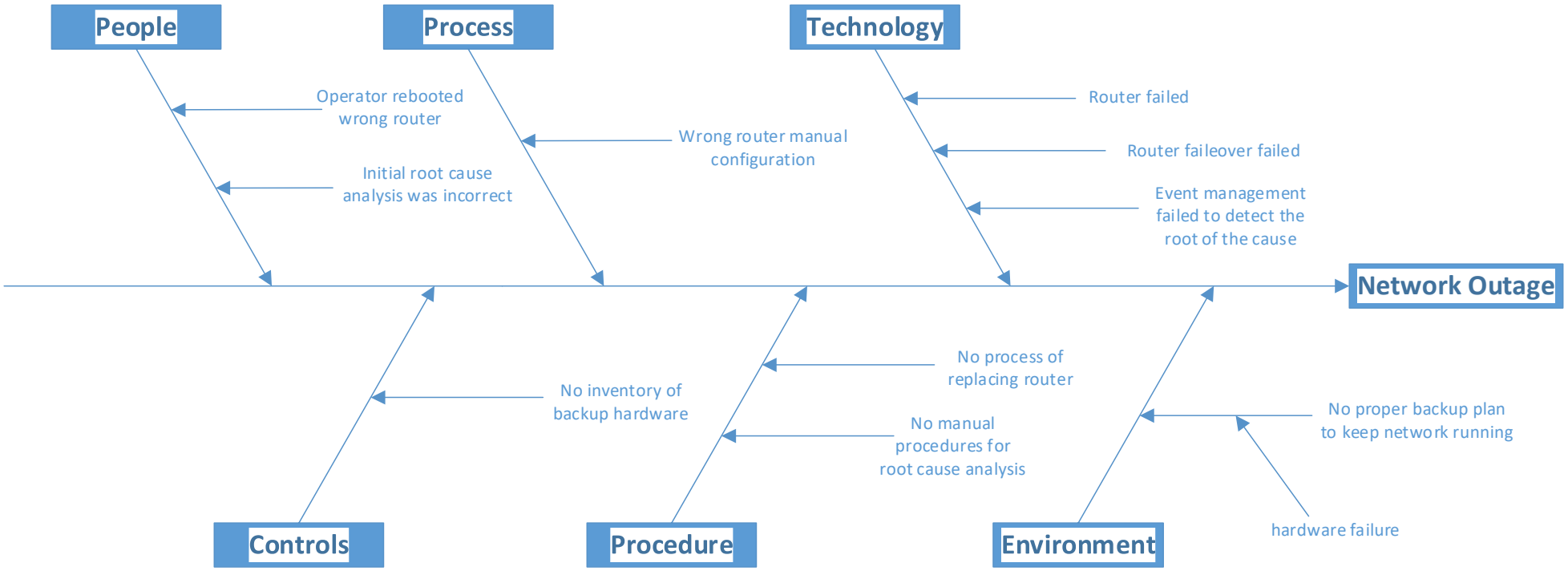
Muhammad Izham Bin Norhamadi
B032020039

d.



Muhammad Izham Bin Norhamadi
B032020039

e.



Muhammad Izham Bin Norhamadi
B032020039

Question 3

a.

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**

   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**

   Having technologies that can monitor the network environment of a company can considerably aid in the detection of new threats.

4. **Prepare an incident response plan**

   An incident response plan helps organization do as much as possible to remain proactively prepared so the security team can move quickly and efficiently to remediate any issues

5. **Implement firewall and antivirus software**

   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

Muhammad Izham Bin Norhamadi
B032020039

b.

1. **Develop an Effective Security Strategy**

   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.

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.

Muhammad Izham Bin Norhamadi
B032020039

c.

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

a.

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.

Muhammad Izham Bin Norhamadi
B032020039

b.

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

Muhammad Izham Bin Norhamadi
B032020039

c.

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