Task 1

Based on learning activities:

If an organisation has three information assets to evaluate for risk management purposes (as shown in the accompanying data) which vulnerability should be evaluated for additional controls first? Which vulnerability should be evaluated last?

Data:

1. *Switch L47 connects a network to the Internet. It has two vulnerabilities: susceptibility to hardware failure, with a likelihood of 0.4, and susceptibility to an SNMP buffer overflow attack, with a likelihood of 0.2. This switch has an impact rating of 90 and has no current controls in place. There is a 60 percent certainty of the assumptions and data.*
2. *Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has Web server software that is vulnerable to attack via invalid Unicode values. The likelihood of such an attack is estimated at 0.2. The server has been assigned an impact value of 100, and a control has been implemented that reduces the impact of the vulnerability by 60 percent. There is an 75 percent certainty of the assumptions and data.*
3. *Operators use the MGMT45 control console to monitor operations in the server room. It has no passwords and is susceptible to unlogged misuse by the operators. Estimates show the likelihood of misuse is 0.1. There are no controls in place on this asset, which has an impact rating of 5. There is a 90 percent certainty of the assumptions and data.*

Asset 1 hardware failure susceptibility:

90 x 0.4 = 36

0% of 90 = 0

40% of 90 = 14.4

36 - 0 + 14.4 = 50.4

Vulnerability 1 rated as 50.4 = (90 × 0.4) – 0% + 40%

Asset 1 SNMP buffer overflow attack susceptibility:

90 x 0.2 = 18

0% of 90 = 0

40% of 90 = 14.4

18 - 0 + 14.4 = 25.2

Vulnerability 2 rated as 25.2 = (90 × 0.2) – 0% + 40%

Asset 2 invalid Unicode value vulnerability:

100 x 0.2 = 20

60% of 40 = 12

25% of 40 = 5

20 - 12 + 5 = 13

Vulnerability 3 rated as 13 = (100 × 0.2) – 60% + 25%

Asset 3 unlogged misuse susceptibility:

5 x 0.1 = 0.5

0% of 0.5 = 0

10% of 0.5 = 0.05

0.5 - 0 + 0.05 = 0.55

Vulnerability 4 rated as 0.55 = (5 × 0.1) – 0% + 10%

Based on the above data and calculations, Asset 1's (Switch L47) susceptibility to hardware should be addressed first. Asset 3's (MGMT45 control console) vulnerability (susceptibility to unlogged misuse) should be addressed last.

Task 2

In terms of controlling risk:

Identify what is meant by Defence, Transference, Mitigation, Acceptance and Termination and how they tie into the Ranked Vulnerability worksheet? Provide a couple of bullet points per topic.

Based on explanations provided by Whitman and Mattord (2019) -

Defence - the application of controls/safeguards to eliminate/reduce remaining risk:

- The preferred risk treatment strategy, also known as "avoidance". Most common approaches for adoption are:
    - Application of policy;
    - Application of security education, training and awareness (SETA) programs;
    - Implementation of technology.
- Forms part of the risk assessment equation as the "current controls" factor, and would have a direct impact on the outcome of the assessment in the Ranked Vulnerability Risk Worksheet (RVRW).

Transference - "transferring" risks to assets, areas or entities external to those conducting the risk assessment:

- Not without risk in itself, this is effectively outsourcing risk. If implemented, it should be in combination with an effective SLA to ensure the required level of security is in place.
- Often used when organisations do not have the knowledge/skills/resources to address the risk identified. Approach does not reduce the risk, only transfers the responsibility for it.

Mitigation - reducing the likely impact in the instance of a vulnerability successfully being exploited

- Employed using effective contingency planning. Includes four types of plans:
    - Incident Response;
    - Disaster Recovery;
    - Business Continuity;
    - Crises Management.
- Impacts the impact rating element of the risk assessment equation - employing an effective mitigation risk treatment strategy would lower the impact rating, thereby lowering the resulting risk-rating factor.

Acceptance - making an informed decision to take no action to address an asset's residual risk level:

- To adopt this risk treatment strategy is to accept the outcome from any exploitation of a vulnerability that has been identified, and must be a conscious decision.

- Acceptance of a risk should be adopted only when the following information has been assessed:
    - Level of risk to the asset (part of the RVRW - risk-rating factor);
    - Probability/likelihood of a successful attack (part of the RVRW);
    - Damage or loss that could result from a successful attack (part of the RVRW - asset impact);
    - Cost benefit analysis.

Termination - removing an asset from the operating environment:

- Not simply the abandonment of an asset (this would classify as an acceptance of the risk instead).
- This strategy will remove the risk entirely from the enterprise (and consequently from the RVRW) and must be a conscious decision made following a thorough risk assessment of the asset.

Task 3

What is achieved by the CBA in terms of managing risk? Provide 4/5 bullet points.

Based on explanations provided by Mattord and Whitman (2019) -

- Attempts to quantify "the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages" (Mattord and Whitman, 2019, p. 380).
- The value of an asset to an organisation can be determined using its cost or its actual/perceived benefit to the organisation.
- Most commonly used approaches for quantifying a value figure for information assets:
    - Value retained from the cost of creating the information asset;
    - Value retained from past maintenance of the information asset;
    - Value implied by the cost of replacing the information;
    - Value from providing the information;
    - Value acquired from the cost of protecting the information;
    - Value to owners;

    - Value of intellectual property;
    - Value to adversaries;
    - Loss of productivity while the information assets are unavailable;
    - Loss of revenue while information assets are unavailable;
    - Total cost of ownership.
- Resulting value of information asset is compared to the cost of implementing and maintaining a control to mitigate the risk to the asset. The organisation can then make an informed decision about whether the benefit gained from implementing the control is equal to or greater than the cost of implementing the same control.
- Results of a CBA are rendered irrelevant in instances where there exists a legal requirement to protect information held by an information asset.