

# 5-2 Project Three Milestone: Prioritizing Evaluation Criteria

andree salvo

Southern New Hampshire University

CYB 220

Instructor: Wesley Buchan

## CYB 220 5-2 Project Three Milestone: Prioritizing Evaluation Criteria

### Operational Frame (Business Context)

- **Organizational Attributes:** the specific set of organizational attributes that define how a company executes its day-to-day activities, focusing on core processes, workflows, and systems needed to deliver a product or service efficiently, essentially encompassing the "how" of achieving strategic goals at the ground level; key attributes include clearly defined roles, standardized procedures, performance metrics, and a focus on operational efficiency and effectiveness within the organization's structure.
- **Organizational Constraints:** refers to any internal or external factors that limit or restrict a company's ability to operate effectively, including limitations on resources like finances, workforce skills, technology, or even regulatory environments, essentially acting as obstacles that hinder the achievement of organizational goals; these constraints can be related to inadequate training, poor equipment, conflicting demands, lack of information, or insufficient support from other team members, essentially impacting employee performance and overall operational efficiency.

### Technology Evaluation Criteria Table:

Complete the blank column in the technology evaluation criteria table in the provided worksheet. Use the manager's questions and the evaluation criteria to identify relevant company profile information for 10-13 evaluation criteria from the organizational security plan material in the scenario.

Evaluation Factor	Evaluation Criteria	Manager's Questions Aligned to Criteria	Relevant Organizational Security Plan Information (From Scenario)
Effectiveness	Ability to identify network-connected systems	1.a. What are the organizational attributes?	Organizational attributes refer to the 4 network segments, which have 150-200 hosts, giving access between different segments based on user roles and responsibilities.
		2.a.i. What is the level of concern about who's on (or off) the network?	Depending on the level of who is "on or off," the network is critical. Employees or yourself must know whether you or someone else will be on the network or off it.
Effectiveness	Ability to discern operating systems of network-connected systems	1.b. What are the organizational constraints?	All host has to run on the same exact Operating system.
		2.a.ii. What is the level of concern about detailed information relating to specific assets on (or off) the network?	The level of concern is high. The reason is that the organization needs to have detailed information about each asset. It ensures the network stays secure and runs smoothly, so that only the right people are using it correctly. Organizations don't want anything to be changed, so that in a way, nothing causes harm within its network.
Effectiveness	Ability to discern specific software applications based on their unique data flows	1.a. What are the organizational attributes?	The software is the same everywhere in the organization. Everyone is expected to use the same software and applications, it helps keep everything easier to manage.
		1.b. What are the organizational constraints?	Each segment uses the same software.
		2.a.iii. What is the level of concern about the ability to defeat secure communications?	The level of concern is high, everything must be encrypted and protected.

		2.a.v. What is the level of concern about potential for harm?	The level of concern is high -- data could potentially be lost, damaged, or stolen.
Effectiveness	Ability to handle encrypted data flows	1.b. What are the organizational constraints?	The same software would be used on all segments.
		2.a.iii. What is the level of concern about the ability to defeat secure communications?	Level of concern is high, reason being is because data must be encrypted and protected by every possible means.
		2.a.v. What is the level of concern about potential for harm?	The level of concern is extremely high because it is a risk. Data should always be kept safe and secure.
Effectiveness	Reliability under stress	1.b. What are the organizational constraints?	Every segment's number of hosts would be an organizational limitation.
		2.a.iv. What is the level of concern about resilience?	The concern is high because of the many hosts compared to the five people doing the monitoring.
Effectiveness	Potential to cause individual network-connected system outage	1.b. What are the organizational constraints?	None, since there are enough hosts to maintain a fully functioning system while the IT team solves the issue.
		2.a.iv. What is the level of concern about resilience?	The level of concern would be high because there are only 5 staff members inside the department.
		2.a.v. What is the level of concern about potential for harm?	There's not much to worry about because there's really no security risk if a host happens to go down.
Effectiveness	Potential to cause individual network-connected system disruption/slowdown	1.a. What are the organizational attributes?	The organizational capacity is full. it has plenty of hosts to handle the accommodation of each and every one of its employees.
		2.a.i. What is the level of concern about who's on (or off) the network?	Concerns are low. Several other hosts can still be used.
		2.a.v. What is the level of concern about potential for harm?	Concerns are low, because if one host goes down the rest will be fine.
Effectiveness	Potential cause of network outage	1.a. What are the organizational attributes?	Four segments with 150-200 hosts.
		2.a.i. What is the level of concern about who's on (or off) the network?	Medium, the network should support every user who's on or off the network.
		2.a.iii. What is the level of concern about the ability to defeat secure communications?	High, an unauthorized user who would potentially gain access to the networks.
		2.a.iv. What is the level of concern about resilience?	Medium, it depends on how many employees are in the organization. It can be fixed quickly.
Effectiveness	Potential cause of network disruption/slowdown	1.a. What are the organizational attributes?	Four segments with 150-200 hosts.
		2.a.i. What is the level of concern about who's on (or off) the network?	Medium, the network should support every user who's on or off the network.

		2.a.iii. What is the level of concern about the ability to defeat secure communications?	The level of concern is high. Unauthorized users gaining access could cause disruptions or slowdowns.
		2.a.iv. What is the level of concern about resilience?	The level of concern is medium. Fewer employees, the longer the wait time to fix.
Effectiveness	Potential cause of excessive alerts	1.b. What are the organizational constraints?	Four segments with 150-200 hosts.
		2.a.i. What is the level of concern about who's on (or off) the network?	Medium, the network should support every user who's on or off the network.
		2.a.iii. What is the level of concern about the ability to defeat secure communications?	None, communications are low.
Cost	Software	1.a. What are the organizational attributes?	Four segments with 150-200 hosts with different software.
		1.b. What are the organizational constraints?	All hosts must be handled by the network at the same time, and employees must be associated with the hosts.
		2.b.i. Can we afford the investment?	Yes we can afford it if everything is working properly.
		2.b.ii. Do we have the right people to implement?	Employees who are properly trained and have the necessary skills and knowledge. Yes we would have the right people to implement.
Cost	Personnel (training)	1.a. What are the organizational attributes?	Two experienced professionals, two new hires, and I as a trainee
		1.b. What are the organizational constraints?	Less because the professionals can guide and instruct the trainee (me).
		2.b.i. Can we afford the investment?	Indeed, it is mandatory since workers are already receiving funds.
		2.b.ii. Do we have the right people to implement?	Yes, since there are enough skilled professionals to train the newly.
Cost	Deployment (time to implement)	1.a. What are the organizational attributes?	Four segments with 150-200 hosts.
		1.b. What are the organizational constraints?	Maintenance should only be on Sundays
		2.b.ii. Do we have the right people to implement?	No, we would have to bring more IT professionals due to the cost.
		2.b.iii. Will it take too much time?	Yes, it would take some time.
Cost	Deployment (complexity)	2.b.iv. Is the tech/activity too complex?	Indeed, it needs to be done correctly.
		1.b. What are the organizational constraints?	Downtime should be scheduled on Sundays for maintenance.
		2.b.ii. Do we have the right people to implement?	With proper training and skilled professionals, we should have the right people to implement without any hassle.
		2.b.iv. Is the tech/activity too complex?	Yes, the complexity would take a bit of time to do a network reconfiguration.

### Evaluation Criteria Priority List

Based on your assessment of the relevant information from the organizational security plan, and provide a **prioritized list** of the three most important evaluation criteria from column #2 of the Technology Evaluation Criteria Table above. Justify your rationale for determining the priority of your selected elements.

1.	<b>False Positives</b>
2.	<b>Network Effects</b>
3.	<b>Time</b>
<b>Justification:</b> Describe why you selected the three evaluation criteria above as the most important based on your analysis of the scenario situation in the space below.	
<i>False positives can lead to false alerts if you're using IDS/IPS, and can lead to alert fatigue. It can also delay real-time threat responses. Network effects. Networks should be monitored daily because we don't want an unauthorized user to gain access to the network, and we need to see who's going to be on or off. Lastly, Time. Performance or upgrades should be scheduled for Sunday for maintenance, so that there are no issues occurring.</i>	

### Fundamental Security Design Principles

Select two **Fundamental Security Design Principles** from the CYB 220 Glossary that best encompass your Evaluation Criteria Priority List in the table above. Explain the correlation between your Evaluation Criteria Priorities (identified in the table above) and the two **Fundamental Security Design Principles** you chose.

1.	<i>Defense in depth</i>
2.	<i>Least Privilege</i>
<b>Explanation of Correlation:</b> Explain the correlation between your Evaluation Criteria Priorities (identified in the table above) and the two Fundamental Security Design Principles you chose in the space below.	
<b>Defense in Depth</b> provides multiple layers of protection to protect critical assets so that if one layer fails, there are others to help keep critical information safe. <b>Least Privilege</b> is important because it gives users only a certain level of access to perform a task that is required. If an account is compromised, this reduces the risk of having any real damage done.	