Performing a Qualitative Risk Assessment for an IT Infrastructure

Course Name and Number: ITN 262

Student Name: Afeefah Manzoor

Instructor Name: KK

Lab Due Date: 9/4/20

1: What is an IT risk assessment’s goal or objective?

An IT risk assessment is use to identify risks and evaluate the risks on the analysis the vulnerabilites and threats. These risks then are prioritized based on their importance, severity, and impact.

2: Why is it difficult to conduct a quantitative risk assessment for an IT infrastructure?

It can be hard to quantify it because these are just opinions of experts.

3: What was your rationale in assigning a “1” risk impact/risk factor value of “Critical” to an

identified risk, threat, or vulnerability?

A "1" is given to a risk/threat/vulnerability, mean that the impact can place the organization at an increased liability.

4: After you had assigned the “1”, “2”, and “3” risk impact/risk factor values to the identified risks,

threats, and vulnerabilities, how did you prioritize the “1”, “2”, and “3” risk elements? What

would you say to executive management about your final recommended prioritization?

1= Critical, meaning the organization is placed at an increased liability

2=Major, meaning the CIA of the organization's IT infrastructure and intellectual property assets were impacted.

3= Minor, meaning that the user or employee's productivity or availability of the IT infrastructure were impacted.

5: Identify a risk-mitigation solution for each of the following risk factors:

1. User downloads and clicks on an unknown e-mail attachment

a: -effective emailing attachment filtering and restrictions

1. Workstation OS has a known software vulnerability

b: -periodic workstation domain vulnerability testing

1. Need to prevent eavesdropping on WLAN due to customer privacy data access

c: -WLAN network keys that require password for wireless connections/access

-require second level authentication before granting WLAN access

-turn off broadcasting of WAPs

1. Weak ingress/egress traffic-filtering degrades performance

d: -apply WAN optimization and data compression solutions for accessing remote systems

1. DoS/DDoS attack from the WAN/Internet

e: -apply filter on exterior IP stateful firewalls

-alert ISP provider

1. Remote access from home office

f: - apply first level and second level security for remote access to sensitive system/applications/data

1. Production server corrupts database

g: -implement daily backups of data

- off-site data storage for archiving monthly

- define data recover procedures.