Student:	Email:
Kaleb Alstott	alstottk1@mymail.nku.edu

Time on Task:	Progress:
2 hours, 26 minutes	100%

Report Generated: Tuesday, October 12, 2021 at 10:20 PM

Guided Exercises

Part 1: Prepare for a Risk Assessment

4. Given the scenario provided above, **identify** the level of the risk assessment you will perform. Your risk assessment may cover multiple tiers.

The level in which these risk assessments will be performed in tiers of 1 and 2 which are, tier 1: organization, and tier 2: mission and business process.

5. For three of the five vulnerabilities identified in the scenario provided above, **identify** the Tier that would best address the vulnerability and provide your justification.

Vulnerability - Critical vulnerabilities exist on servers due to a lack of patch management procedures. The tier this would fall under and be addressed would be in tier 2. I believe this is in tier two of the pyramid level because in tier two mission and business processes are handled and since we are not organizing which is tier 1 it is only right for this vulnerability to fall into tier 2. Vulnerability 2- stroing critical information on clear text files that are easily accessible. This vulnerability would be placed in tier 1 due to how this is all about how you protect and store your data correctly. Dealing with tier 1 its all about organization and here is where this vulnerability should be placed. Vulnerability 3- Inactive test accounts that have been in the server for longer than 90 days. This would fall into tier 2, this is because we are dealing with systems involved in the company and business that need to reworked.

7. **Describe** the purpose of this risk assessment.

"Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support" The goal and the purpose for this risk assessment here is to be able to prioritize and identify risk in which we would hand to a top level management position.

9. **Describe** the scope of this risk assessment.

The scope of this risk assessment has to deal with the ACME corporation. We would handle all the assets such as hardware, software, employee training, etc.

11. **Identify** the assumptions and constraints associated with this risk assessment.

Dealing with many assumptions and constraints for a risk assessment can be very challenging. To start any type of natural disaster that takes place will not be identified in the risk assessment. Also in the risk assessment obvious constraints may be a time management of the project.

13. **Identify** the information sources associated with this risk assessment.

The information sources we would need is access to test accounts, user passwords for modification, company documents of monitoring and testing that has occurred, access to patch notes and procedures, etc.

21. Based on the information provided above, **define** your assessment approach as quantitative, qualitative, or semi-quantitative and **provide** your justification.

The assessment approach I think we would use would be Qualitative. I think this because when dealing with Likelihood, and impact, these values are represented in a chart or by objects rather than numbers to back this information up.

Part 2: Conduct a NIST SP 800-30 Risk Assessment

2. Think about the sort of adversarial agent that could exploit the vulnerability summarized above. **Identify** one threat source according to Table D-2 on Page D-2 of the NIST SP800-30 document.

One threat source according to Table D-2 on Page D-2 of the NIST SP800-30 document is an obvious outsider.

3. For the selected threat, **identify** its capability, intent, and targeting, according to Table D-3, Table D-4, and Table D-5, respectively.

Dealing with an outsider capability- moderate, "has moderate resources, expertise, and opportunities to support multiple successful attacks." intent- high, "The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure." targeting- moderate, "The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information."

4. For the selected threat, **identify** specific threat event(s) according to Table E-2.

Specific threat events according to table e-2, would be exploiting recently discovered data vulnerabilities, performing malware detection, network sniffing, exploiting unauthorized informations to users, etc.

5. **Identify** the vulnerability and **determine** the vulnerability severity, according to Table F-2.

The vulnerability found was the outsider, and when we take all consideration in such as the capability, intent, threat source and much, id consider the vulnerability severity to be very high.

6. **Identify** the *Likelihood of threat event initiation* and *Likelihood of threat event resulting in adverse impacts* values, according to Table G-2 and Table G-4, respectively.

When looking at the tables of g-2 and g-4 I would like to say the Likelihood of threat event initiation would be high, the Likelihood of threat event resulting in adverse impacts values would also be high.

7. **Identify** the overall likelihood value, which you will later use in SimpleRisk, according to Table G-5.

The overall likelihood value would be high. When you look at the table g-5, high X high = high.

8. **Identify** the potential adverse impacts, according to Table H-2.

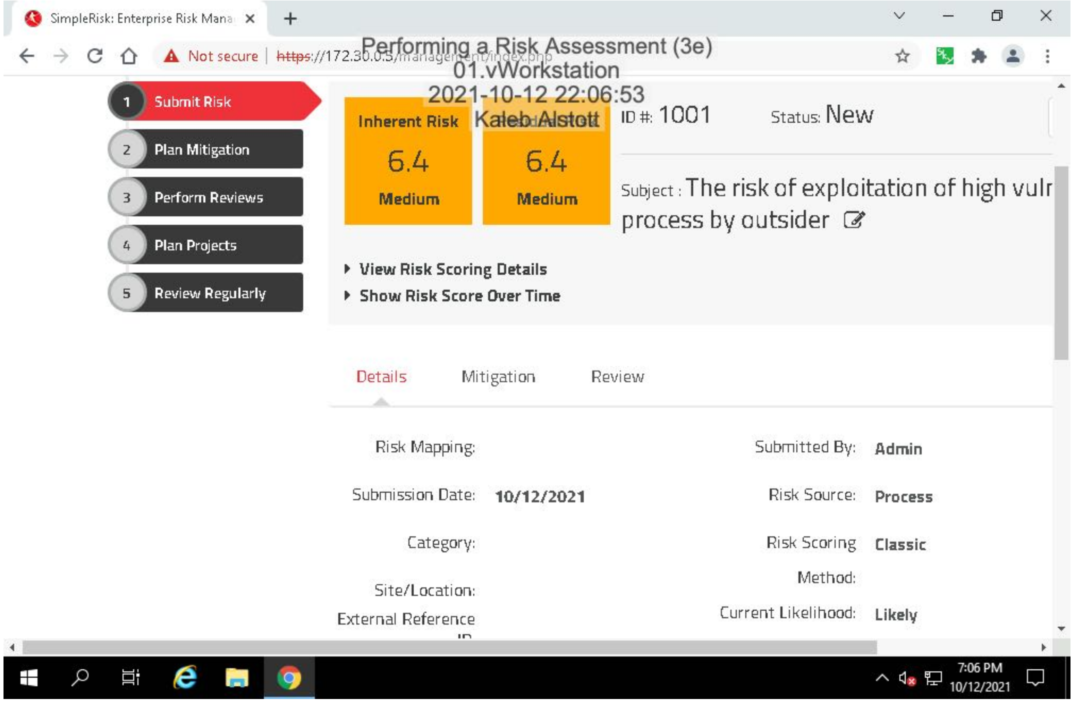
Potential adverse impacts according to table h-2 can be damage to image or reputation, identity theft, loss of intellectual property, direct financial costs, etc.

9. **Identify** the impact value, which you will later use in SimpleRisk, according to Table H-3.

The overall impact value according to table h-3, would be high

Part 3: Use SimpleRisk to Track and Calculate Risk

8. **Make a screen capture** showing the **submitted risk in SimpleRisk.**


SimpleRisk: Enterprise Risk Mana
Not secure | ~~https~~://172.30.0.5/management/index.php
1 Submit Risk
2 Plan Mitigation
3 Perform Reviews
4 Plan Projects
5 Review Regularly
View Risk Scoring Details
Show Risk Score Over Time
Details
Mitigation
Review
7:06 PM
10/12/2021

Performing a Risk Assessment (3e)
01.vWorkstation
2021-10-12 22:06:53
Kaleb Alstott

Inherent Risk 6.4 Medium

6.4 Medium

ID #: 1001 Status: New

Subject : The risk of exploitation of high vulr process by outsider

Risk Mapping:

Submission Date: 10/12/2021

Category:

Site/Location:

External Reference ID

Submitted By: Admin

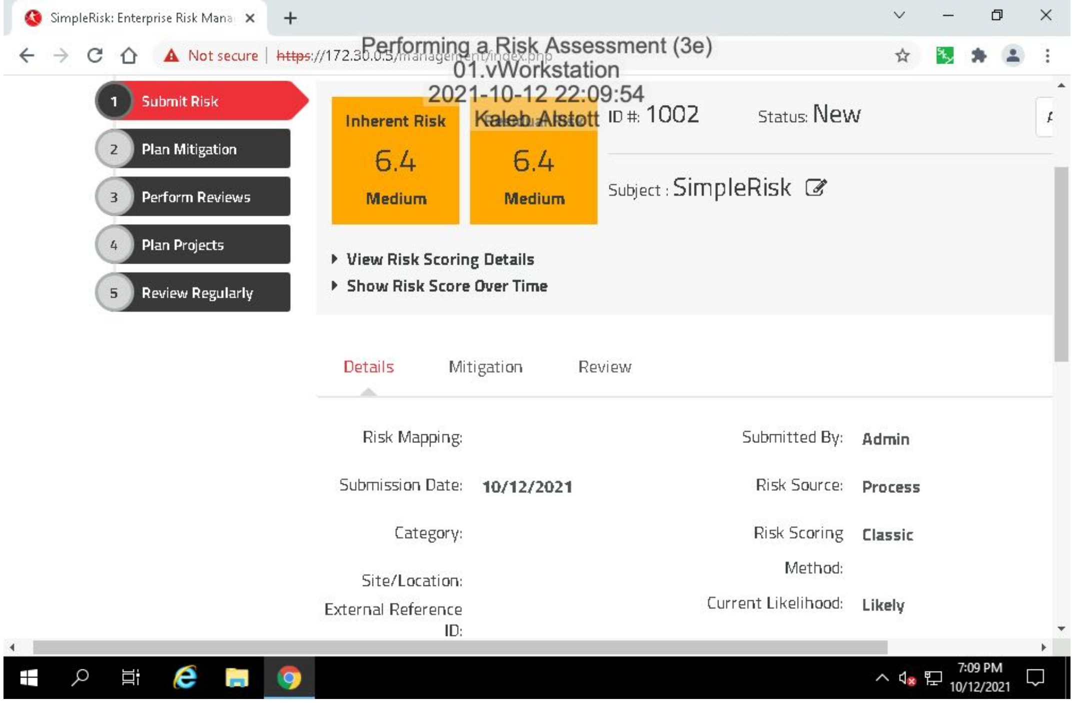
Risk Source: Process

Risk Scoring Method: Classic

Current Likelihood: Likely

Challenge Exercise

Make a screenshot showing the **submitted risk for Target in SimpleRisk.**



Performing a Risk Assessment (3e)
01.vWorkstation
2021-10-12 22:09:54
Kaleb Alstott

Inherent Risk 6.4 Medium

Residual Risk 6.4 Medium

ID #: 1002

Status: New

Subject : SimpleRisk

View Risk Scoring Details

Show Risk Score Over Time

Risk Mapping:

Submission Date: 10/12/2021

Category:

Site/Location:

External Reference ID:

Submitted By: Admin

Risk Source: Process

Risk Scoring Method: Classic

Current Likelihood: Likely

Explain your choices and thought process.

My through process and choices when taking into account of this SimpleRisk would be simply trying to find vulnerabilities and causes of why this may be. The big cause of this was caused back in 2013 with the target data breach. After this vulnerability it seems like we have came across new threats such as malicious IP addresses, and harmful emails. When taking all of these vulnerability's into a Simple risk plan we can see how it can be a very likely and high probability of this happening.