Student:	Email:
Patrick Kierzkowski	pxk405@francis.edu

Time on Task:	Progress:
18 hours, 45 minutes	100%

Report Generated: Monday, July 7, 2025 at 9:39 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 of my risk assessment would cover all three levels, Organization, Mission/Business Processes, and Information Systems.

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.

A production server has been discovered to contain a test account created when the server was in a staging environment. The same server contains user accounts that had been inactive for more than 90 days. The most important discovery was that the IT department has not assigned an individual or team to manage the administration of user accounts: This would be mission/business because it's a failure in operational security controls in the business side.
Critical vulnerabilities exist on servers due to a lack of patch management procedures: This would be information systems because it is a technical vulnerability in the IT branch. Acme has not been regularly monitoring and testing its IT infrastructure is also information systems because its a system security issue that comes from the IT of acme.

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

The purpose of this risk assessment is to minimize risks that can be a potential vulnerability down the line to Acme. You want to identify potential risks and evaluate them before they become an issue. Based on what you find you prioritize them based on the threat they have

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

The scope of the risk assessment is that it covers Acme's organizational policies, business processes and the IT department to identify and mitigate risks. Specifically it would address things like the way they enforce their policies, operational security controls and system monitoring.

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

It is assumed that Acme already have other policies in place, even if they're weak or out of date. Some more assumptions are that they will have full access to documents regarding the companies policies .There would also be constraints, and some constraints would be the budget, time, and compliance with employees in Acme.

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

The information sources associated with this risk assignment are Acme's security policies, their IT department, and user account data. Audit logs and system reports could also be used to identify the potential vulnerabilities.

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

It is qualitative because it focuses on identifying vulnerabilities and evaluating security policies, while relying on judgment, not on numbers. If the risk assessment was based on the numbers, it would have been quantitative.

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.

An outsider, such as a hacker could exploit this vulnerability because they can take advantage of no regular monitoring and testing.

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

Capability: High. The hacker would have strong technical skills and an understanding of the systems vulnerabilities, so they could exploit it.
Intent: High. It is malicious intent and seeks to have a presence for a while, as they don't test and monitor the infrastructure.
Targeting: High. To exploit the system and vulnerability so they can get access to sensitive info such as user logins and system data

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

Perform reconnaissance and gather information.Gather information using open source discovery oforganizational information.Perform perimeter network reconnaissance/scanning.Craft phishing attacks.Craft spear phishing attacks.Deliver known malware to internal organizational information systems

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

The vulnerability is the organizations failure to regularly monitor and test the systems. This could lead to potential exploits as they can take advantage without detection. The vulnerability assessment would be high because critical systems could be exploited without anyone knowing. The lack of regular monitoring makes it easy for these attacks to go unnoticed. The severity would be an 8

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.

Likelihood of threat event initiation is 8/High
Likelihood of threat event resulting in adverse impacts values is 10/Very high

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

Very high/10

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

Inability to perform current missions/business functions
Damage to trust relationships, as well as reputation |

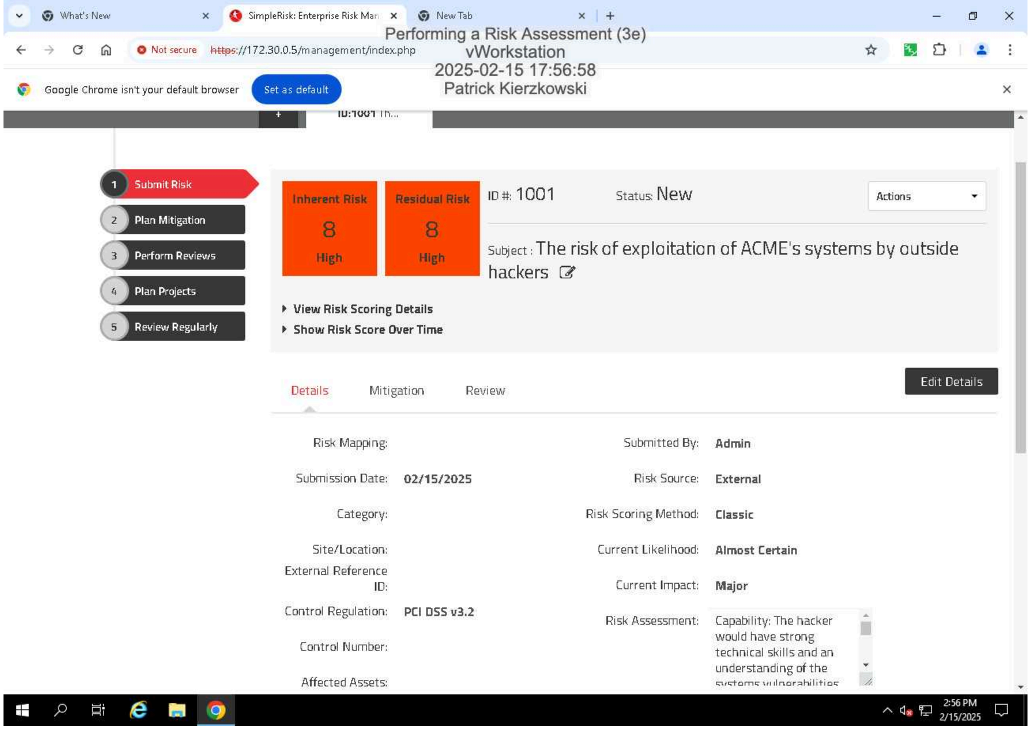
Damage to or loss of information systems or networks
Loss of intellectual property
Loss of Personally Identifiable Information
Damage to or incapacitation of a critical infrastructure sector

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

High/8

Part 3: Use SimpleRisk to Track and Calculate Risk

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



Inherent Risk: 8 High

Residual Risk: 8 High

ID #: 1001

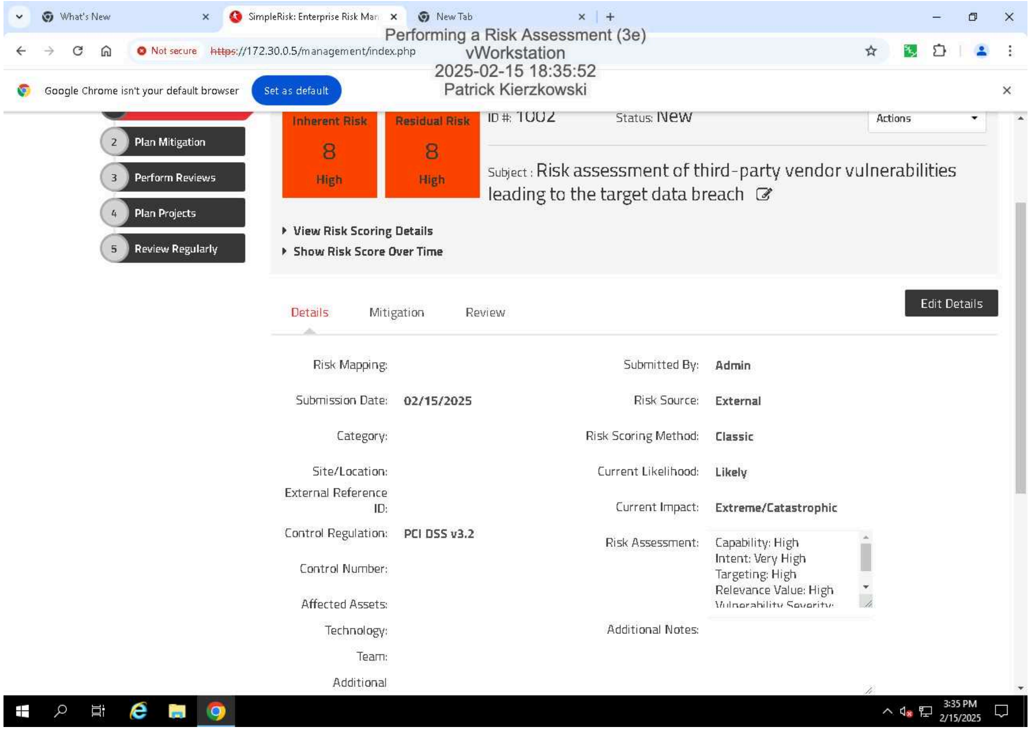
Status: New

Subject : The risk of exploitation of ACME's systems by outside hackers

Risk Mapping:		Submitted By:	Admin
Submission Date:	02/15/2025	Risk Source:	External
Category:		Risk Scoring Method:	Classic
Site/Location:		Current Likelihood:	Almost Certain
External Reference ID:		Current Impact:	Major
Control Regulation:	PCI DSS v3.2	Risk Assessment:	Capability: The hacker would have strong technical skills and an understanding of the systems vulnerabilities
Control Number:			
Affected Assets:			

Challenge Exercise

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



Performing a Risk Assessment (3e)
vWorkstation
2025-02-15 18:35:52
Patrick Kierzkowski

Inherent Risk 8 High

Residual Risk 8 High

ID #: 1002

Status: New

Subject : Risk assessment of third-party vendor vulnerabilities leading to the target data breach

Risk Mapping:

Submission Date: 02/15/2025

Category:

Site/Location:

External Reference ID:

Control Regulation: PCI DSS v3.2

Control Number:

Affected Assets:

Technology:

Team:

Additional

Submitted By: Admin

Risk Source: External

Risk Scoring Method: Classic

Current Likelihood: Likely

Current Impact: Extreme/Catastrophic

Risk Assessment: Capability: High
Intent: Very High
Targeting: High
Relevance Value: High
Vulnerability Severity:

Additional Notes:

Explain your choices and thought process.

Capability: High. Used good skills and tactics. They were able to map networks and exploit vendor systems, shows they were experienced.
Intent: Very high. Wanted to steal data, personal info. Wanted moneyTargeting: High. They targeted a third party vendor called Fazio, a weak link in their security.
Relevance value: The vulnerability in the vendor's security was responsible for the breachVulnerability Severity: The lack of real-time monitoring and security controls allowed attackers to access Target's systems, making the severity high.Current Impact: It would be very high and lead to big financial loss and damage to targetCurrent likelihood: Likely if the poor vendor security and phishing attacks remain exploitable