

GRC200-M4-1-Assignment-Risk Management Simulation

[Start Assignment](#)

Due No Due Date **Points** 30 **Submitting** a file upload **Attempts** 0
Allowed Attempts 1

Exercise Objective(s)

By the end of this lab, the student should be able to:

- ⊗EO1: Define why risk communication is important.
- ⊗EO2: Discuss risk communication strategy and principles.
- ⊗EO3: Describe the Risk Register.
- ⊗EO4: Utilize the Risk Register.

Abstract

This GRC200 Project is about identifying cyber-risks and the controls that can be used to mitigate them. Maintaining and updating information about risks an organization faces is a core function of the GRC team. This exercise presents a simple case study in the health care domain. As you examine this case, you are to use the information provided in the case to identify some risks, build an (abbreviated) risk register for a selection of risks, and identify controls that can mitigate the identified risks.

Submission: This assignment is the continuation of the **GRC200-M3-1-Lab-Risk Management Simulation** (<https://learning.flatironschool.com/courses/6144/assignments/205856>) and will be your final assessment for GRC200.

Case Study


Organizational Summary

Zombie Health System – ZHS, is a 501-c3 (Not for Profit) healthcare organization that currently has over 25,000 patients, 2000 privileged physicians and other medical team members with authorization to practice medicine in the organization, and 800 administration and staff, 50 of which are IT and Security team members.



Your team is the GRC IT Security advisor group responsible for all things Governance, Risk, and Compliance within the digital environment of the healthcare organization. Your team reports to the Chief Legal Officer, Mr. Clicker, and works closely with the legal counsel and audit team, as well as the rest of the staff reporting to the CIO and CISO.

Scenario

OCR released a recent report of security incidents and data breaches ([here](https://www.hhs.gov/sites/default/files/controlling-access-epi-newsletter.pdf) ) (<https://www.hhs.gov/sites/default/files/controlling-access-epi-newsletter.pdf>) that found that

61% of analyzed data breaches in the healthcare sector were perpetrated by external threat actors and 39% by insiders. Without appropriate authorization policies and procedures and access controls, hackers, workforce members, or anyone with an Internet connection may have impermissible access to the health data, including protected health information (PHI), that HIPAA regulated entities hold. News stories and OCR investigations abound of hackers infiltrating information systems, workforce members impermissibly accessing patients' health information, and electronic PHI (ePHI) being left on unsecured servers.

In response to these very disturbing statistics, the ZHS board of directors has decided to support research for new ways of protecting our employees and the 25,000 patient records. The directives are for the GRC IT Security advisors to create a NIST risk assessment of all identified risk register items and suggest NIST controls to mitigate the identified risks, bringing the risk down to an acceptable level based on the Risk Matrix.

Activity

Risk Register

Create a NIST risk assessment of all identified risk register items and suggest NIST controls to mitigate the identified risks, bringing the risk down to an acceptable level based on the Risk Matrix.

Please use brainstorming to generate an initial list of items. Here are some areas that you can use to get started. This list is not exhaustive:

- Identity Access Management
- Vendor Management (Contract Liability Risk): 27800 records x cost per record for simple liability calculation.
- Access Controls
- SIEM and log review
- Web App Security
- Vulnerability Management

You can determine the costs of vendor management liability risk using this **report**

(<https://learning.flatironschool.com/courses/6144/files/3397604?wrap=1>). ↓

(https://learning.flatironschool.com/courses/6144/files/3397604/download?download_frd=1) from IBM.

Using this template **Risk Register**

(<https://learning.flatironschool.com/courses/6144/files/3397603?wrap=1>). ↓

(https://learning.flatironschool.com/courses/6144/files/3397603/download?download_frd=1) ,

identify 3-5 risk items. Specify the level of impact and likelihood using this **impact matrix**

(<https://learning.flatironschool.com/courses/6144/files/3397471?wrap=1>). ↓

(https://learning.flatironschool.com/courses/6144/files/3397471/download?download_frd=1) . The list you generate should have risk items representing each level of risk: Significant, Moderate, and Minor.

Risk Assessment

Using the Enterprise Risk Management (ERM) workflow you learned in the lectures, conduct a full risk assessment on the identified risk items you included in your Risk Register for the Zombie Healthcare System organization.

Use the provided **NIST Control Catalog**

(<https://learning.flatironschool.com/courses/6144/files/3397609?wrap=1>)_ ↓

(https://learning.flatironschool.com/courses/6144/files/3397609/download?download_frd=1) for the Risk Treatment of Mitigation. The **NIST CSF to HIPPA Crosswalk resource**

(<https://learning.flatironschool.com/courses/6144/files/3397602?wrap=1>)_ ↓

(https://learning.flatironschool.com/courses/6144/files/3397602/download?download_frd=1) may help you identify additional risks and gaps in your risk management program. Once the controls are applied to the digital environment, evaluate each risk item using the **NIST Risk**

Assessment Procedures ([https://learning.flatironschool.com/courses/6144/files/3397608?](https://learning.flatironschool.com/courses/6144/files/3397608?wrap=1)

[wrap=1](https://learning.flatironschool.com/courses/6144/files/3397608/download?download_frd=1))_ ↓ ([https://learning.flatironschool.com/courses/6144/files/3397608/download?](https://learning.flatironschool.com/courses/6144/files/3397608/download?download_frd=1)

[download_frd=1](https://learning.flatironschool.com/courses/6144/files/3397608/download?download_frd=1)) for the calculation of the residual risk to determine if layering of controls will be necessary or if the residual risk is acceptable on the Risk Matrix scale.

Once you are satisfied that you have identified all the items, evaluated and logged the controls, and identified and mitigated the risk to an acceptable level, summarize your information for the ZHS leadership team.

Reporting






Your report to the leadership team should be a presentation using slides. Include

- A GRC team introduction
- Risk Register with a summary of the risks
- NIST Controls explaining the controls used and their effectiveness.

Conclude with your explanation of the GRC recommendations for any future risk mitigation needed.

Submission: Submit your Risk Register spreadsheet and your presentation to ZHS's leadership team.

References

- **Summer 2021 OCR Cybersecurity Newsletter: Controlling Access to ePHI: For Whose Eyes Only? - PDF**  (<https://www.hhs.gov/sites/default/files/controlling-access-ephi-newsletter.pdf>)
- **HHS-OCR Cyber Attack Checklist 06-2017 - PDF**
(<https://learning.flatironschool.com/courses/6144/files/3396989?wrap=1>) 
(https://learning.flatironschool.com/courses/6144/files/3396989/download?download_frd=1)
- **IBM Cost of a Data Breach Report 2021 - PDF**
(<https://learning.flatironschool.com/courses/6144/files/3397604?wrap=1>) 
(https://learning.flatironschool.com/courses/6144/files/3397604/download?download_frd=1)
- **NIST-CSF-to-HIPPA-Security-Crosswalk - PDF**
(<https://learning.flatironschool.com/courses/6144/files/3397602?wrap=1>) 
(https://learning.flatironschool.com/courses/6144/files/3397602/download?download_frd=1)
- **NIST-SP800-53ar5-Assessment-Procedures - Excel**
(<https://learning.flatironschool.com/courses/6144/files/3397608?wrap=1>) 
(https://learning.flatironschool.com/courses/6144/files/3397608/download?download_frd=1)
- **NIST-SP800-53r5-Control-Catalog - Excel**
(<https://learning.flatironschool.com/courses/6144/files/3397609?wrap=1>) 
(https://learning.flatironschool.com/courses/6144/files/3397609/download?download_frd=1)

Criteria	Ratings			Pts
Introduction What is this presentation and why important?	4 pts Excellent Short summary of Risk Management process and value to the organization.	3 pts Good Summary of Risk Management process but does not apply to the organization.	1 pts Weak Summary of findings but does not introduce Risk Management process.	4 pts
Risk Register – Data Risk Register data capture.	5 pts Excellent Risk Register captures information on 4 or more risk items. Description, priority, owner, dependent systems, and other fields completed with good information.	3 pts Good Risk Register captures information on 2-3 risk items. Description, priority, owner, dependent systems, and other fields mostly completed with acceptable information.	1 pts Weak Risk Register captures information on 1-2 risk items. Roughly half or less of fields completed OR information in a few cells seems suspect.	5 pts
Risk Register – Analysis Risk Register analysis of risks.	5 pts Excellent Risk Register includes an excellent analysis of each risk listed, including priority from impact/likelihood, cost, risk treatment, NIST control, residual risk, risk accepted or not.	3 pts Good Risk Register includes an analysis data about each risk listed, including some but not all of: priority from impact/likelihood, cost, risk treatment, NIST control, residual risk, risk accepted or not.	1 pts Weak Risk Register analysis of priority, cost, treatment, and residual risk is incomplete for most or all the Risk items listed.	5 pts
Presentation of Risks Presentation of Risks	5 pts Excellent Presentation of risks to leadership includes summary of all risks studied and highlights about risks of concern. Presentation includes an excellent summary of overall risk to the organization.	3 pts Good Presentation of risks to leadership includes list of all risks studied and basic information about risks of concern. Presentation may include a summary of overall risk to the organization.	1 pts Weak Presentation of risks to leadership fails to accurately capture information included in the Risk Register AND fails to report on overall risk to the organization.	5 pts

Criteria	Ratings			Pts
Conclusions Findings from this activity.	4 pts Excellent Short, succinct restatement of Risk Management presentation from this report.	3 pts Good Basic restatement of Risk Management recommendations.	1 pts Weak List of Risk Management recommendations.	4 pts
GRC Team Introduction Introduce the team and its function.	2 pts Excellent Information about GRC Team's role and introduction to GRC staff found in presentation.	1 pts Good Information about GRC Team's role and introduction to GRC staff found in presentation.	0 pts No Points No information about the GRC team or GRC staff found.	2 pts
Source List Included?	1 pts Yes Source list included.	0 pts No Points No source list found.		1 pts
Presentation Language Language use, writing, and editing of submission.	4 pts Excellent Presentation organized, well written, has professional appearance.	2 pts Good Useful presentation but lacking professional polish.	0 pts No Points Presentation needs improvement to make it easier to read.	4 pts
Total Points: 30				

Have specific feedback?

Tell us here! ([https://flatironschoolforms.formstack.com/forms/canvas_feedback?](https://flatironschoolforms.formstack.com/forms/canvas_feedback?CourseID=6144&LessonID=205858&LessonType=assignments&CanvasUserID=10700&Course=None)

[CourseID=6144&LessonID=205858&LessonType=assignments&CanvasUserID=10700&Course=None](https://flatironschoolforms.formstack.com/forms/canvas_feedback?CourseID=6144&LessonID=205858&LessonType=assignments&CanvasUserID=10700&Course=None))