Managing Enterprise Cybersecurity MIS 4596

Class 9

Milestone 1 Review with Guidance for Milestone 2

Report Content and Grading

1. **Title Page and Header/Footer**
2. **Executive Summary**
3. **Table** – Breach of Security Objectives of Financial Information Management Data Types and Risk Impacts to Organizational Operations, Assets, or Individuals
4. **Section 1** – Security Objectives for Financial Information Management Systems Data Types
5. **Section 2** – Risk Impact Categories for breaches of Security Objectives
6. **Section 3** – Risk Impact Categories for breaches of Security Objectives for Financial Information Management Systems Data Types
7. **References**
8. **Glossary**

Grading Rubric and Distributions – Section 1

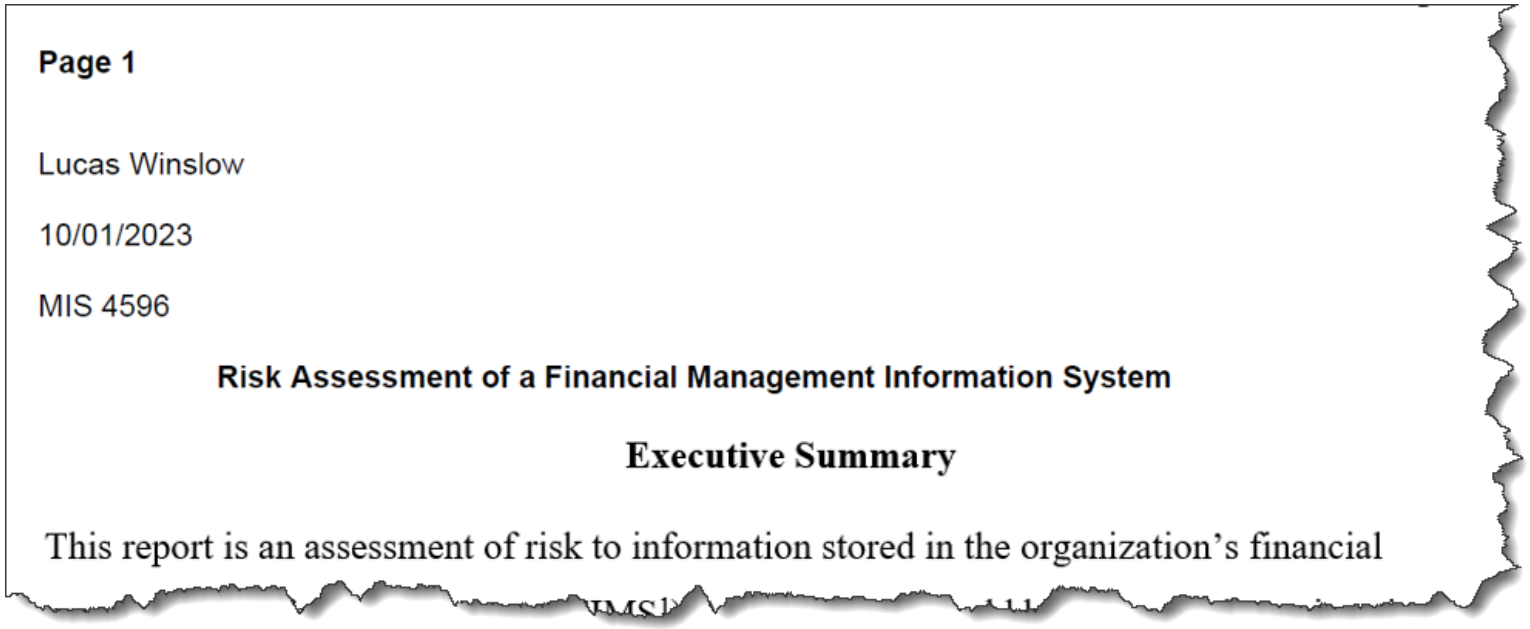
Title Page and Header/Footer						Executive Summary						Table				Section 1					Section 2					Section 3								Grade	
Student Name	Report Name	Date	Course	Page #s	Total	Goal of Paper	IS Type	Impact of Breach on Organization	Explaination of Impact	Introduce Report Sections	Total	Contents of Table	Table Title	Table Description	Total	Section #	Section Title	Intro	Define CIA Security Objectives	Total	Section #	Section Title	Intro	Define Impact Categories	Total	Section #	Section Title	Intro	Info Type Security Categorization	Explain Categorization and Impacts	Total	References	Glossary	Total Score	Numeric Grade
5	3	1	0.5	0.5	10	10	5	5	5	5	30	10	5	5	20	5	5	5	10	25	5	5	5	10	25	5	5	5	5	5	25	5	0	140	
5	3	1	0.5	0.5	**10**	10	5	5	5	5	**30**	10	5	4	**19**	5	4	4	8	**21**	5	4	4	8	**21**	5	0	4	5	4	**18**	5	5	**129**	**92%**
5	3	1	0.5	0	**9.5**	10	5	4	4	4	**27**	10	4	3	**17**	5	4	3	8	**20**	5	4	4	8	**21**	5	4	4	4	4	**21**	3	0	**118.5**	**85%**
5	3	1	0.5	0.5	**10**	8	5	0	0	5	**18**	10	4	4	**18**	5	4	4	9	**22**	5	5	4	8	**22**	5	5	4	4	4	**22**	3	0	**115**	**82%**
5	3	1	0.5	0.5	**10**	8	4	0	0	4	**16**	10	4	4	**18**	5	5	4	8	**22**	5	4	4	8	**21**	5	3	3	5	2	**18**	5	5	**115**	**82%**
4	3	1	0	0.5	**8.5**	9	5	2	2	5	**23**	10	4	5	**19**	5	4	4	8	**21**	5	4	4	8	**21**	5	4	1	4	5	**19**	3	0	**114.5**	**82%**
5	0	1	0.5	0	**6.5**	10	5	5	5	3	**28**	10	4	3	**17**	5	4	3	8	**20**	5	4	3	8	**20**	5	3	0	4	5	**17**	4	0	**112.5**	**80%**
5	3	1	0	0	**9**	7	5	0	3	4	**19**	10	4	4	**18**	5	5	3	8	**21**	5	4	3	8	**20**	5	4	4	3	4	**20**	5	0	**112**	**80%**
5	3	1	0.5	0	**9.5**	7	0	0	0	4	**11**	10	4	3	**17**	5	4	3	8	**20**	5	4	3	8	**20**	5	3	3	4	3	**18**	3	0	**98.5**	**70%**
0	3	0	0	0	**3**	8	4	1	3	3	**19**	10	4	3	**17**	5	4	4	8	**21**	5	4	3	7	**19**	5	2	0	4	4	**15**	4	0	**98**	**70%**
0	3	0	0	0	**3**	8	3	0	2	3	**16**	10	4	4	**18**	5	4	4	7	**20**	5	4	3	8	**20**	5	0	4	4	4	**17**	4	0	**98**	**70%**
0	0	0	0	0	**0**	9	5	5	2	3	**24**	10	3	4	**17**	5	5	3	8	**21**	5	4	3	8	**20**	5	3	0	0	3	**11**	4	0	**97**	**69%**
5	0	0	0	0.5	**5.5**	8	5	0	0	0	**13**	10	4	3	**17**	5	5	3	8	**21**	5	4	4	8	**21**	5	4	0	4	3	**16**	3	0	**96.5**	**69%**
5	3	1	0	0	**9**	9	3	5	3	1	**21**	10	4	4	**18**	5	5	1	8	**19**	5	4	1	8	**18**	2	0	0	0	4	**6**	5	0	**96**	**69%**
5	0	1	0.5	0	**6.5**	8	4	0	2	4	**18**	10	2	3	**15**	5	0	1	8	**14**	5	0	1	8	**14**	5	0	1	4	4	**14**	5	0	**86.5**	**62%**
0	3	0	0	0	**3**	8	4	0	1	3	**16**	10	4	4	**18**	5	0	3	7	**15**	5	0	3	8	**16**	5	0	4	3	3	**15**	3	0	**86**	**61%**
5	2	1	0	0	**8**	9	4	0	3	0	**16**	10	4	3	**17**	5	0	1	8	**14**	5	0	1	8	**14**	5	0	0	3	3	**11**	5	0	**85**	**61%**
5	2	1	0.5	0.5	**9**	7	5	0	3	0	**15**	10	0	3	**13**	5	0	3	8	**16**	5	0	3		**8**	5	0	3	4	4	**16**	4	0	**81**	**58%**
0	2	0	0	0.5	**2.5**	7	4	0	2	0	**13**	10	5	4	**19**	0	4	0	7	**11**	0	4	0	7	**11**	0	4	3	7	3	**17**	2	0	**75.5**	**54%**
5	2	0	0	0	**7**	8	4	2	3	0	**17**	1	0	1	**2**	5	0	1	8	**14**	5	0	2	8	**15**	5	0	1	0	4	**10**	3	0	**68**	**49%**
0	2	0	0	0	**2**	7	4	2	3	0	**16**	1	0	0	**1**	0	0	0	2	**2**	0	0	0	2	**2**	0	0	0	3	3	**6**	5	0	**34**	**24%**

Grading Rubric and Distributions – Section 3

Title Page and Header/Footer						Executive Summary						Table				Section 1					Section 2					Section 3								Grade	
Student Name	Report Name	Date	Course	Page #s	Total	Goal of Paper	IS Type	Impact of Breach on Organization	Explaination of Impact	Introduce Report Sections	Total	Contents of Table	Table Title	Table Description	Total	Section #	Section Title	Intro	Define CIA Security Objectives	Total	Section #	Section Title	Intro	Define Impact Categories	Total	Section #	Section Title	Intro	Info Type Security Categorization	Explain Categorization and Impacts	Total	References	Glossary	Total Score	Numeric Grade
5	3	1	0.5	0.5	10	10	5	5	5	5	30	10	5	5	20	5	5	5	10	25	5	5	5	10	25	5	5	5	5	5	25	5	0	140	
5	3	1	0	0.5	**9.5**	9	5	2	2	4	**22**	10	4	5	**19**	5	4	5	8	**22**	5	4	4	8	**21**	5	4	0	4	4	**17**	5	0	**115.5**	**83%**
5	3	1	0	0	**9**	9	5	0	0	5	**19**	10	4	4	**18**	5	4	4	8	**21**	5	4	4	8	**21**	5	4	4	4	4	**21**	4		**113**	**81%**
5	3	0	0.5	0	**8.5**	8	5	0	1	4	**18**	10	4	4	**18**	5	4	3	8	**20**	5	4	4	8	**21**	5	4	4	4	4	**21**	5	0	**111.5**	**80%**
5	3	0	0	0.5	**8.5**	8	4	4	3	3	**22**	10	4	5	**19**	5	4	3	8	**20**	5	4	4	8	**21**	5	4	2	0	4	**15**	4	0	**109.5**	**78%**
0	3	0	0	0.5	**3.5**	10	5	5	3	5	**28**	10	4	4	**18**	5	4	3	8	**20**	5	4	3	8	**20**	5	4	0	4	3	**16**	4	0	**109.5**	**78%**
5	3	1	0	0.5	**9.5**	10	4	5	4	5	**28**	10	4	4	**18**	5	4	3	8	**20**	5	4	4	8	**21**	0	0	0	4	4	**8**	4	0	**108.5**	**78%**
0	3	0	0	0	**3**	10	5	5	4	0	**24**	10	4	4	**18**	5	4	3	8	**20**	5	4	3	8	**20**	5	4	0	4	4	**17**	3	0	**105**	**75%**
5	3	1	0	0	**9**	8	5	3	3	5	**24**	10	0	4	**14**	5	4	4	8	**21**	5	4	0	8	**17**	5	4	0	0	4	**13**	4	0	**102**	**73%**
5	2	1	0.5	0	**8.5**	8	4	0	0	0	**12**	10	5	4	**19**	5	4	3	8	**20**	5	4	4	8	**21**	5	4	0	0	4	**13**	5	0	**98.5**	**70%**
5	2	1	0.5	0.5	**9**	8	5	0	0	0	**13**	10	0	3	**13**	5	4	0	8	**17**	5	4	0	8	**17**	5	4	0	4	4	**17**	5	4	**95**	**68%**
5	3	1	0	0	**9**	9	5	5	1	0	**20**	10	4	4	**18**	5	0	2	8	**15**	5	0	2	8	**15**	5	0	3	0	4	**12**	4	0	**93**	**66%**
5	3	1	0.5	0.5	**10**	8	4	0	0	0	**12**	10	4	4	**18**	5	0	2	8	**15**	5	0	2	7	**14**	5	0	3	4	4	**16**	4	0	**89**	**64%**
5	3	1	0.5	0	**9.5**	8	4	0	0	4	**16**	10	4	1	**15**	5	0	3	8	**16**	5	0	3	8	**16**	5	0	0	3	4	**12**	4	0	**88.5**	**63%**
5	3	1	0.5	0	**9.5**	8	4	0	3	0	**15**	10	4	4	**18**	5	0	3	8	**16**	5	0	3	8	**16**	0	0	0	0	4	**4**	3	4	**85.5**	**61%**
5	1	0	0.5	0	**6.5**	8	4	0	0	2	**14**	10	4	3	**17**	4	4	0	8	**16**	4	4	0	8	**16**	4	4	0	0	4	**12**	4	0	**85.5**	**61%**
5	2	1	0.5	0.5	**9**	8	5	0	0	0	**13**	10	4	3	**17**	5	0	2	7	**14**	5	0	2	8	**15**	5	0	0	2	4	**11**	4	0	**83**	**59%**
5	2	1	0.5	0	**8.5**	8	5	0	1	0	**14**	10	4	4	**18**	0	0	3	8	**11**	0	4	2	8	**14**	0	4	0	3	4	**11**	2	2	**80.5**	**58%**
5	2	1	0.5	0	**8.5**	8	5	0	1	0	**14**	10	4	0	**14**	5	0	0	8	**13**	5	0	2	8	**15**	5	0	1	0	4	**10**	5	1	**80.5**	**58%**
5	1	1	0	0	**7**	8	4	0	0	1	**13**	10	0	0	**10**	5	0	3	8	**16**	5	0	3	8	**16**	5	0	0	0	4	**9**	3	0	**74**	**53%**
3	2	0	0.5	0.5	**6**	8	4	0	1	0	**13**	2	4	1	**7**	5	0	2	8	**15**	5	0	2	8	**15**	5	0	0	5	3	**13**	0	0	**69**	**49%**
					0						**0**				**0**					**0**					**0**						**0**			**0**	**0%**

Title Page and Header/Footer

Student Name	Report Name	Date	Course	Page #s	Total
5	3	1	0.5	0.5	10



Page 1

Lucas Winslow

10/01/2023

MIS 4596

Risk Assessment of a Financial Management Information System

Executive Summary

This report is an assessment of risk to information stored in the organization's financial

Executive Summary

Goal of Paper	IS Type	Impact of Breach on Organization	Explaination of Impact	Introduce Report Sections	Total
10	5	5	5	5	30

Executive Summary

This report is an assessment of risk to information stored in the organization's financial management information system (FIMS[1]). Management should be aware of the serious impacts that could affect the organization's assets, operations, and individuals if there is a security breach in six of the types of information stored in the FIMS. If there is a breach in confidentiality, the information type that has the greatest risk is funds control. If there is a breach in integrity, the information types that have the greatest risk are reporting and information, funds control, accounting, payments, collections and receivables, and cost accounting and performance management.

Section 1 of this report explains in more detail about the security objectives that were established by FISMA[2]. These security objectives are confidentiality, integrity, and availability. Section 2 of this report defines the three levels of impact that can affect the organization's assets, operations, and individuals. These impact levels are low, moderate, and high. Section 3 of this report takes both the security objectives and impact levels for each FIMS type and explains in detail how it would affect the organization's assets, operations, and individuals.

Table

In this report, we have included a table in which the information types are listed with a corresponding impact rating based on how serious the effects could be if there is a data breach. Column A lists out the information type. Columns B, C, and D have an impact rating based on the security objectives of confidentiality, integrity, and availability, respectively. Column E lists the overall impact rating for each information type row (2-8). At the bottom of column E, the overall impact rating of the FIMS is listed, highlighted in yellow. This table will be referred to throughout the report as Table 1.

	A	B	C	D	E
1	**Information Type**	**Confidentiality**	**Integrity**	**Availability**	**Overall Impact Rating**
2	Asset and Liability Management	Low	Low	Low	Low
3	Reporting and Information	Low	Moderate	Low	Moderate
4	Funds Control	Moderate	Moderate	Low	Moderate
5	Accounting	Low	Moderate	Low	Moderate
6	Payments	Low	Moderate	Low	Moderate
7	Collections and Receivables	Low	Moderate	Low	Moderate
8	Cost Accounting/ Performance Measurement	Low	Moderate	Low	Moderate
9	**Information System Categorization:**	Moderate	Moderate	Low	Moderate

Table 1. Information Type Security Risk Classification

We rely on the National Institute of Standards and Technology (NIST) to help us understand that there are seven types of information that may be stored in the organization's FIMS. In the table above, referred to as "table 1", those information types are listed with a corresponding impact rating based on how serious the effects could be if there is a data breach for each information type. These impact ratings come from NIST Special Publication 800-60 Volume II.

Contents of Table	Table Title	Table Description	Total
10	5	5	20

Section 1

Section #	Section Title	Intro	Define CIA Security Objectives	Total
5	5	5	10	25

Section I: Security Objectives: Confidentiality, Integrity, and Availability

There are three security objectives identified in columns B, C, and D in table 1 for information and information systems. The first objective, confidentiality, is the unauthorized disclosure of information. This security objective protects the privacy of personal or confidential information. The second objective, integrity, is the unauthorized modification or destruction of information. As you will read in this report, unauthorized modifications to the information can lead to implications for the company, depending on the classification of risk. The final security objective, availability, is the disruption of access to the information. These security objectives were established by the Federal Information Security Management Act of 2002, or FISMA. This report explains the impact that a security breach could have for each of these objectives.

	A	B	C	D	E
1	**Information Type**	**Confidentiality**	**Integrity**	**Availability**	**Overall Impact Rating**
2	Asset and Liability Management	Low	Low	Low	Low
3	Reporting and Information	Low	Moderate	Low	Moderate
4	Funds Control	Moderate	Moderate	Low	Moderate
5	Accounting	Low	Moderate	Low	Moderate
6	Payments	Low	Moderate	Low	Moderate
7	Collections and Receivables	Low	Moderate	Low	Moderate
8	Cost Accounting/ Performance Measurement	Low	Moderate	Low	Moderate
9	**Information System Categorization:**	Moderate	Moderate	Low	Moderate

Table 1. Information Type Security Risk Classification

Section 2

Section #	Section Title	Intro	Define Impact Categories	Total
5	5	5	10	25

Section II: Potential Impact Ratings of a Cyber Breach on Organizations and Individuals

The FIPS 199[3] defines three levels of impact that a company could face if there is a breach of data stored in the FIMS. These are defined as low, moderate, and high. These are found in columns B, C, and D of Table 1. If the potential impact is *low*, there could be a limited effect on the organizational operations, assets, and individuals. If the potential impact is *moderate*, there could be a serious effect on the organization's operations, assets, and individuals. Finally, if the potential impact is *high*, there could be a catastrophic or severe effect on the organization. Each information type and security objective have a recommended rating based on the impacts identified above.

Section 3

Section #	Section Title	Intro	Info Type Security Categorization	Explain Categorization and Impacts	Total
5	5	5	5	5	25

Section III: Financial Management Information Types and Cybersecurity Breach Impact Ratings

Financial management identifies the accounting practices and procedures that assist in the accurate reporting and handling of company revenues, expenditures, funding, and more. The financial management information system has an overall impact rating of *moderate* . This means that if there is a security breach, there could be a serious adverse effect on the organizational operations, assets, or individuals of an organization. For example, a security breach could result in serious damage to organizational assets or financial loss. It is important that management understand the potential impacts of breaches of financial information types in terms of the cybersecurity objectives. In the following sections, we will identify these ratings for each information type starting with funds control.

Funds Control: Moderate Impact (Serious Adverse Effect)

The overall impact rating for the funds control information type is moderate, meaning a breach would have a serious adverse effect on organizational assets, operations, and individuals. This is because while availability has a low impact level, confidentiality and integrity have moderate impact levels. Confidentiality breaches were assigned a moderate impact because certain funds control information like budgets and performance outcomes give important insight into operations and unauthorized

References and Glossary – with examples

References	Glossary
5	0

https://www.nist.gov/nist-research-library/reference-format-nist-publications

References

National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS PUBS) 199, https://doi.org/10.6028/NIST.FIPS.199, Accessed 2 Feb. 2023.

National Institute of Standards and Technology (2010) Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. (U.S. Department of Commerce, Washington, D.C.), NIST Special Publication (NIST SP) 800-60 Vol. 2, Rev. 1, https://doi.org/10.6028/NIST.SP.800-60v2r1, Accessed 2 Feb. 2023.

Glossary

Availability: This security objective aims to ensure that critical information and systems remain accessible and reliable even in the event of a security breach of the financial information system.

Adverse effect: The harmful consequences that may arise from a security breach, such as damage to reputation, legal complications, and financial losses. These outcomes can be categorized as limited, serious, or catastrophic.

Confidentiality: The security objective of preventing unauthorized entities from viewing confidential or sensitive information in the case of a breach in the financial information system.

FIPS Publication 199: A guideline that defines the three impact ratings of confidentiality, integrity, and availability, which are used to categorize information and information systems.

Impact rating: A measure of potential harm that can result from a security breach. It is assigned to specific information types and security objectives and is classified as low, moderate, and high depending on the severity of the impact.

Integrity: This security objective is to prevent the unauthorized alteration or destruction of data and ensure the completeness and accuracy of information if the financial information system experiences a breach.

NIST Special Publication 800-60 Volume II: A guide from the National Institute of Standards and Technology that classifies information systems based on the potential impacts of a security breach.