Milestone 4 Instructions

Your assignment is to create a risk assessment and mitigation report for managers of a (fictitious) company who owns and depends on financial management information and information system running on the server you examined in the penetration test you conducted in Milestone 2.

The purpose of your risk assessment is to clarify the level of concern for confidentiality, integrity, and availability and the potential impact on the business' operations should the information and information system be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction.

Your risk assessment will be based on:

1. Security objectives and potential impacts defined in Federal Information Processing Standard 199: "Standards for Security Categorization of Federal Information and Information Systems",
2. Methodology for assigning impact levels to information and information system types described in NIST Special Publication 800-60 Volume I,
3. Provisional security categorizations assigned to the financial management information types by NIST Special Publication 800-60 Volume II,
4. Determination of an overall security categorization for the financial management information system based on the provisional security categorization of the information types (from 3 above)

The security risk categorization you present in your risk assessment will enable you to use NIST Special Publication 800-53r4 to select security controls to mitigate the vulnerabilities you identified in your penetration test report of Milestones 2 and 3. for the financial management information and information system.

To start, consider that the Milestone 2 server was an integral part of processing the following financial management information types (e.g., the C.3.2 "Financial Management" category in Table 6 of NIST Special Publication 800-60 Volume I):

- Asset and Liability Management (C.3.2.1)

- Reporting and Information (C.3.2.2)
- Funds Control (C.3.2.3)
- Accounting (C.3.2.4)
- Payments (C.3.2.5)
- Collections and Receivables (C.3.2.6)
- Cost Accounting/ Performance Measurement (C.3.2.7)

Objectives

1. For each information type listed in section C.3.2 of NIST Special Publication 800-60 Volume II, follow the guidance for categorizing the security objectives for the information type such as Asset and Liability Management in the first row of the table below. For each information type also determine an Overall Categorization for the information and complete the categorization of the other financial management information types in the remaining rows of the table:

Information Type	NIST SP 800-60 ID	Confidentiality	Integrity	Availability	Overall Categorization
Asset and Liability Management	C.3.2.1	Low	Low	Low	Low
Reporting and Information	C.3.2.2				
Funds Control	C.3.2.3				
Accounting	C.3.2.4				
Payments	C.3.2.5				
Collections and Receivables	C.3.2.6				
Cost Accounting/ Performance Measurement	C.3.2.7				
	Information System Categorization:				

   Then determine the summary categorization for the financial management information system in the bottom row under "Confidentiality," "Integrity," and "Availability". Determine and record the Overall Categorization.

   You can use the Excel spreadsheet file available here as a template.

2. For each information type, use the information and in FIPS-199: "Standards for Security Categorization of Federal Information and Information Systems" (particularly Table 1) to help you understand how to describe the potential impact to the organization if the Milestone 2 server containing these financial management information types and was breached.
3. For each weakness you identified in Section 3 of your penetration test report, research controls that mitigate these weaknesses which are identified in Table D-2: "Security Control Baselines" from NIST Special

Publication 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations". You may also use other outside sources such as NIST's Framework for Improving Critical Infrastructure Cybersecurity.

Explain and justify in your assessment how these controls would mitigate each vulnerability finding you identified in Milestone 2.

Written Report Deliverable

You should write the report for a managerial audience, one that is not versed in information security concepts. In other words, you need to explain the concepts in terms that can be easily understood by managers without technical experience. If you use technical or unfamiliar terms, include a glossary of the terms used.

The suggested length requirement for the report is 10 pages, but your report must not exceed 15 pages (not including appendices).

In writing your report, organize for a decision making executive. This means you should discuss the most serious vulnerabilities first.

Report Sections

1. Executive summary (1 page). In this section, state that the report:
    - Is an assessment of risk to information stored on financial management systems, part of which is the server examined in your penetration test report.
    - Discusses the likelihood that this information will be compromised, given the results of your penetration test report.
    - Explains impacts of different information types on the business, in terms of confidentiality, integrity, and availability, following NIST Special Publication 800-60 Volume II.
    - Explains the potential low, moderate, and high, impacts clearly so that your reader understands their implications in terms of corresponding limited, serious, and severe/catastrophic adverse effects, per FIPS-199: "Standards for Security Categorization of Federal Information and Information Systems" and NIST Special Publication 800-60 Volume II.

    - Proposes controls to mitigate the vulnerabilities identified in your penetration report, in accordance with the Security Control Baselines from NIST Special Publication 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations".
2. In Section 1, briefly summarize the findings of vulnerabilities reported in Section 3 of your penetration test report. *Discuss why the likelihood is high that these vulnerabilities could be exploited in the future*.
3. In Section 2,
    - Present and describe the impact rating table you created in Step 1 above and discuss the impact on the organization of a breach of each of the security objectives for each of the information types.
    - Bold the items in the right-most column of the table to highlight the overall impact rating for each information type.
    - Explain how you determined these impact ratings based on NIST Special Publication 800-60 Volume II.
    - In section 2.1, briefly define confidentiality, integrity and availability, per FIPS 199. You're welcome to quote from FIPS-199: "Standards for Security Categorization of Federal Information and Information Systems" (be sure to cite the source).
    - In section 2.2, briefly define each impact category: "low," "moderate," and "high," and explain their correspondence to "limited," "serious," "severe" or "catastrophic" adverse effects, per FIPS-199: "Standards for Security Categorization of Federal Information and Information Systems".
    - In section 2.3, create a subsection for each information type (e.g., Asset and Liability Management, C.3.2.1).
        - For each subsection, explain why it has the impact rating that it does for confidentiality, integrity, and availability. You're welcome to quote from NIST Special Publication 800-60 Volume II with attribution.
        - Give emphasis to the most serious impacts.
4. In section 3, describe mitigating controls you identified in Step 3 above for the findings of vulnerabilities you reported in Section 3 of your penetration test report.
    - List the specific controls from NIST Special Publication 800-53: "Security and Privacy Controls for Federal Information Systems and

Organizations" (e.g., "IA-2: Identification and Authentication (Organizational Users").
    - Explain each control. You're welcome to quote from NIST 800-53, and NIST Framework for Improving Critical Infrastructure Cybersecurity with attribution.
    - Group your controls by control family (e.g., group all "IA" controls together).
    - *Be explicit how each control would mitigate the vulnerabilities you found*.
5. Add a reference section where you can list the title, author or agency name (e.g., NIST), URL, and access date for the works you cite.