**Milestone 5 Instructions**

*By Drs.*[*Anthony Vance*](https://anthonyvance.com/)

The objective of Milestone 5 is to revise your security assessment report according to the feedback received from the instructor. Polish your draft and focus writing for a managerial, non-technical audience.

The below instructions are repeated from Milestone 4.

 **Objectives**

Your assignment is to create a risk assessment and mitigation report for the server your examined in Milestone 2. However, now consider that the Milestone 3 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](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf)):

* 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](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf), complete a row like the following:



For each row, the “overall impact rating” is the highest impact listed in any of the cells for “confidentiality,” “integrity,” and “availability.”

You can use [this Excel spreadsheet file](https://anthonyvance.com/security-assignments/assets/files/Risk_assessment_table.xlsx) as a template.

1. For each information type, use the information in [FIPS-199: “Standards for Security Categorization of Federal Information and Information Systems”](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf) (particularly Table 1) to write about the potential impact to the organization if the Milestone 2 server was breached containing these information types.
2. For each weakness you identified in Section 3 of your penetration test report, find controls that mitigate these weaknesses from Table D-2: “Security Control Baselines” from [NIST Special Publication 800-53: “Security and Privacy Controls for Federal Information Systems and Organizations”](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).

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

**Written Report Deliverable**

You should write the report for a managerial audience, one that isn’t 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.

There is no length requirement for the report, but your report must not exceed 20 pages (not including appendices).

In writing your report, organize for impact. 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.
	* Classifies impacts to different information types, in terms of confidentiality, integrity, and availability, following [NIST Special Publication 800-60 Volume II](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf).
	* Classifies these potential impacts as “low,” “moderate,” and “high,” which correspond to “limited,” “serious,” “severe” or “catastrophic” adverse effects, per [FIPS-199: “Standards for Security Categorization of Federal Information and Information Systems”](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf).
	* 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”](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).
2. In Section 1, briefly summarize the 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 for each information type.
	* Bold the items in the right-most column.
	* State that these impact ratings come from [NIST Special Publication 800-60 Volume II](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf).
	* In section 2.1, briefly define integrity, confidentiality, and availability, per FIPS 199. You’re welcome to quote from [FIPS-199: “Standards for Security Categorization of Federal Information and Information Systems”](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf).
	* In section 2.2, briefly define each impact category: “low,” “moderate,” and “high,” which correspond to “limited,” “serious,” “severe” or “catastrophic” adverse effects, per [FIPS-199: “Standards for Security Categorization of Federal Information and Information Systems”](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf).
	* 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](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf) with attribution.
		+ Give emphasis to the most serious impacts.
4. In section 3, describe mitigating controls you identified in Step 3 above for the 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”](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) (e.g., “IA-1: Identification and Authentication Policy and Procedures”).
	* Explains each control. You’re welcome to to quote from NIST 800-53, 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.