

ISE 640 Milestone One Guidelines and Rubric

Overview: The milestone assignments in this course directly support you in the completion of your final project, a forensic investigative report. Consider the feedback you have received in class discussions, along with notes you have made in your non-graded investigative journal, to complete this milestone assignment.

This is Milestone One, a draft of Final Project One: Report. The final product will be submitted in Module Nine.

Please note that your non-graded investigative journal will be submitted with this milestone to ensure completion. Make sure that you are adding to your investigative journal as you complete each module.

Prompt: For the summative assessment, you will be taking on the role of a cybersecurity practitioner. You will need to act as a domain expert communicating to a non-expert stakeholder. For this milestone, you will be providing a summary of the scenario from the forensic notes document. You will also be explaining the relevant procedures needed to maintain evidentiary integrity: legal concerns, processes and procedures, and chain of custody. Lastly, you will be explaining details of the investigation, such as resources needed, methods, and findings. Ensure you review the full scenario in the main project document as well as the forensic notes document before drafting your report.

Specifically, the following **critical elements** must be addressed:

- I. **Executive Summary:** Set the stage for your report, providing a brief overview of the situation and the stakeholders who are involved.
- II. **Legal Concerns:** Describe the problem(s) and objectives you are working with the company's attorneys to solve.
- III. **Relevant Procedures:** In this section, you will outline the steps that (hypothetically) you will have to take prior to or as you investigate in order to maintain evidentiary integrity. Use your experiences from other situations you are engaging in within the lab environment to inform your responses.
 - A. **Processes and Procedures:** Describe processes or procedures necessary for handling a criminal situation by an internal employee.
 - B. **Chain of Custody:** Explain how to maintain the chain of custody as you investigate the various aspects of the incident. Support your response with specific examples.
- IV. **Details of Investigation:** Based on your experiences in the labs, there will be specific resources, methods, and tools necessary to support the investigation in the scenario.
 - A. **Resources Needs:** Explain what resources (team knowledge, skills, and abilities) are necessary for gathering the evidence for this forensic investigation. Provide examples based on your experiences from the labs.
 - B. **Methods:** Describe the specific forensic method or approach you used to effectively leverage your available resources.
 - C. **Findings:** Describe the specific findings and the forensic tactics and technologies you employed to reach them.

- V. **Investigative Journal Notes:** Submit your investigative journal that outlines most of the basics from each of the modules upon which you based your notes.

Rubric

Guidelines for Submission: Your assignment should adhere to the following formatting requirements: Write 2 to 3 double-spaced pages using 12-point Times New Roman font and one-inch margins. You should use current APA style guidelines for your citations and reference list. **Be sure to attach both Milestone One and investigative journal files.**

Critical Elements	Proficient (100%)	Needs Improvement (75%)	Not Evident (0%)	Value
Executive Summary	Sets the stage for report, providing a brief overview of the situation and stakeholders involved	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	9
Legal Concerns	Describes the problem(s) and objectives you are working with the company’s attorneys to solve	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	11
Processes and Procedures	Describes processes or procedures necessary for handling a criminal situation by an internal employee.	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	11
Chain of Custody	Explains how to maintain the chain of custody while investigating the various aspects of the incident and supports response with specific examples	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	11
Resources Needed	Explains what resources (team knowledge, skills, and abilities) are necessary for gathering the evidence for this forensic investigation and provides examples based on experiences from the labs	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	11
Methods	Describes the specific forensic method or approach used to effectively leverage available resources	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	11
Findings	Describes the specific findings and the forensic tactics and technologies employed to reach them	Addresses “Proficient” criteria, but there are gaps in clarity, logic, or detail	Does not address critical element, or response is irrelevant	11

Southern New Hampshire University

Critical Elements	Proficient (100%)	Needs Improvement (75%)	Not Evident (0%)	Value
Completion of Investigative Journal	Submits investigative journal that outlines most of the basics from each of the modules upon which notes are based	Submits investigative journal that outlines some basics from each of the modules upon which notes are based	Does not submit investigative journal	15
Articulation of Response	Submission has no major errors related to citations, grammar, spelling, or organization	Submission has some errors related to citations, grammar, spelling, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, or organization that prevent understanding of ideas	10
Total				100%