Southern New Hampshire University

IT 335 Final Project Guidelines and Rubric

Overview

The well-rounded information technology professional will have a sound understanding of the foundational principles of security at the systems level. The final project in this course will provide you with the opportunity to analyze existing and goal security profiles to identify gaps that put organizations at risk. Beyond this, you will also be developing an action plan for addressing identified gaps that will include new or amended policies and plans for implementation. At the heart of this assessment is the knowledge that the ever-changing nature of business and technology requires an ever-evolving, continuously improving pool of information security professionals with organizational perspectives.

Your final project in this course is a report that includes a gap analysis of an organization's security profile in comparison to industry standards and an action plan with recommended policies, adaptations, and considerations for implementation. The project is divided into **six milestones**, which will be submitted at various points throughout the course to scaffold learning and ensure quality final submissions. These milestones will be submitted in **Modules One, Two, Three, Four, Five, and Six. The final submission is due in Module Seven.**

Your assessment will address the following course outcomes:

- IT-335-01: Design policy implementation plans that align to the policy life cycle and ensure continued adherence to information security standards and regulations
- IT-335-02: Propose fundamental information security management policies that address risks, threats, and identified gaps in information security management systems
- IT-335-03: Recommend appropriate controls, guidelines, and principles for promoting effective information security at the technological or mechanism level
- It-335-04: Determine acceptable risk levels at the information security systems level through appraisal of organizational information technology risk postures

Prompt

As a member of a security consultant team, you have been assigned an organization in need of a security review. You have been tasked with performing a security policy gap analysis on the company, for the purposes of comparison to the current security standards established by the International Organization for Standardization (ISO), the leading developer and publisher of international standards spanning any number of topics and industries. Your job is to determine the coverage of these standards that your assigned organization's policies are capable of, and then to make recommendations to fill gaps in security coverage to increase the safety and security of the organization's information. Your recommendations may consist of full new policies, adaptations to existing policies, or a mix of both, as long as you are addressing the gaps you find in your analysis. Your final report will be submitted both to your own supervisor and to the reviewed organization's CEO and board of directors, so remember to use professional language and language that non-IT professionals would understand.

Specifically, while the specific format of your report will follow the guidelines for submission outlined below, the following **critical elements** must be addressed in your report (**not necessarily in the order listed below**):

I. **Executive Summary**: Your executive summary should briefly provide the key points of the report, including why the report was created, the security posture of the organization, and high-level findings and conclusions. This section is similar to an abstract in a traditional APA report; its purpose is to situate the reader and give them a general idea of the purpose, premise, and scope of the report itself. Although this is the opening section of the report, you may wish to complete it last in order to accurately capture the analysis in the body of your report. [IT-335-04]

II. Background, Scope, and Study Overview
   A. **Organizational Background**: Describe the organization (including industry, size, etc.), background, and the reasons consultants were brought in to review its security framework. [IT-335-04]
   B. **Scope**: Identify the scope of the analysis. In other words, what is under review? (For example, is it the whole organizational security framework or specific aspects of the security framework?) [IT-335-03]
   C. **Approach:** Analyze the various policies and detail the approach you took in analyzing the organization's security framework and policies. What did you look at and how did you review the material to determine the security posture? How did you know that this approach would illuminate gaps? [IT-335-02]

III. Gap Analysis and Results
   A. **Security Posture**: What is this organization's security posture? What is the organization's stance on the importance of security, and what level of risk is it willing to accept given the results of your analysis? [IT-335-04]
   B. **Policy Errors and Gaps**: Are there any gaps in the existing policies that you see without comparison to external standards? In other words, are there clear gaps in coverage or policy that could pose potential threats or risks to information and need to be addressed to create a secure framework? These could come in the form of policy errors, policies that are not carried out or shared with the organization as a policy, or many other issues. [IT-335-02]
   C. **Comparison Analysis**: Compare the results of your analysis of the organization's policies and information security framework with the ISO standards to determine gaps in coverage of policy areas. Describe these gaps in coverage. [IT-335-01]
   D. **Technological Analysis**: Information security often relies on the use of technology to implement policies; or alternatively, policies are often created to ensure secure use of technology for storage, sharing, and creating information. For your organization, are there gaps in controls or guidelines that need to be addressed? Are there additional technologies that should be added? Be sure to explain your position. [IT-335-03]

IV. Recommendations
   A. **Findings**: What were your findings at the end of your analysis? What risks, threats, and gaps in coverage did you identify? In other words, to what extent is the organization's information security system deficient or ineffective? [IT-335-03]
   B. **Policies**: Propose new policies or amendments to existing policies to cover the gaps that were identified during your analysis. [IT-335-02]
   C. **Defense:** Defend your policy recommendations. Why are these policies appropriate? What information, whether from the organization, your analysis, or external resources would support the addition of these policies to address the identified gaps? [IT-335-02]

D. **Controls:** What controls, guidelines, and principles would you suggest the company incorporate into its information security system to align to the policies and support a secure information system? Why? [IT-335-03]
E. **Implementation Plan**: How would you propose these policies be implemented to ensure that they are meeting the ISO standards and existing laws and regulations? [IT-335-01]
F. **Policy Life Cycle**: What are your recommendations for ensuring the validity of policies, both your recommended policies and existing policies, over time? In other words, considering the policy life cycle, what would be your recommendation for maintaining these policies to limit policy errors and gaps? [IT-335-01]

Milestones

Milestone One: *Introduction to Wilbur's Widgets*
In **Module One**, you will read the "Wilbur's Widgets Overview" document and turn in a document that outlines the company's background, scope, and security posture. In addition, you will submit five hypothetical questions that you would ask as a security consultant to get a better understanding of the corporation's policy maturity level. **This milestone will be graded using the Milestone One Rubric.**

Milestone Two: *Compliance and Standard Policy Documents*
In **Module Two,** you will compile a comprehensive list of policy documents that need to exist for Wilbur's Widgets. You will need to draft a list of the policies that you plan on using for Wilbur's Widgets' gap analysis document and what purpose these policies serve. To complete this assignment, you may create a table with the policy document needed on one side and the justification for its creation on the other side. **This milestone will be graded using the Milestone Two Rubric.**

Milestone Three: *Create a Policy Implementation Plan*
In **Module Three**, you will create a policy life cycle diagram and a policy implementation plan. You will create the sample policy life cycle diagram to help Wilbur's Widgets' CEO and business users understand the importance of a proper implementation life cycle. In addition to creating the life cycle diagram, you will also create a policy implementation plan, which will help Wilbur's Widgets prepare to implement policies that you will be recommending. **This milestone will be graded using the Milestone Three Rubric.**

Milestone Four: *Policy Exploration*
In **Module Four**, you will submit a sample policy for Wilbur's Widgets. You will need to locate at least two sample organizational policies; with this information, prepare a sample acceptable use policy for Wilbur's Widgets. **This milestone will be graded using the Milestone Four Rubric.**

Milestone Five: *Guideline Development*
In **Module Five**, you will create a guideline document for Wilbur's Widgets that covers how users should store data—both on their computers and in the cloud. This is directly related to Wilbur's Widgets data, and not personal data. **This milestone will be graded using the Milestone Five Rubric.**

Milestone Six: *The Seven Domains of Typical IT Infrastructure*

Southern New Hampshire University

In **Module Six,** you will create a risk flow chart. In addition to creating the risk flow chart, you will need to identify the technological risks for each of the seven IT domains in relation to Wilbur's Widgets. **This milestone will be graded using the Milestone Six Rubric.**

Final Project Submission: *Gap Analysis for Wilbur's Widgets*
In **Module Seven**, you will submit a gap analysis document for Wilbur's Widgets. The gap analysis should be a complete, polished artifact containing all of the critical elements of the final product. It should reflect the incorporation of feedback gained throughout the course. **The final project will be graded using the Final Project Rubric (below).**

Deliverable Milestones

Milestone	Deliverables	Module Due	Grading
1	Introduction to Wilbur's Widgets	One	Graded separately; Milestone One Rubric
2	Standard Policy Documents List	Two	Graded separately; Milestone Two Rubric
3	Create a Policy Implementation Plan	Three	Graded separately; Milestone Three Rubric
4	Policy Exploration	Four	Graded separately; Milestone Four Rubric
5	Guideline Development	Five	Graded separately; Milestone Five Rubric
6	The Seven Domains of IT Infrastructure	Six	Graded separately; Milestone Six Rubric
	Final Product: Gap Analysis for Wilbur's Widgets	Seven	Graded separately; Final Project Rubric

Southern New Hampshire University

Final Project Rubric

Guidelines for Submission: There are strict standards for reporting in this field and your report should adhere to the same professional guidelines and expectations. Your report should be 8–12 pages in length, should follow APA formatting and citation guidelines, and should include the following sections: a title page; an executive summary; a table of contents; background, scope, and overview; findings and recommendations; summary and conclusions; references; and appendices (if necessary for your report; this element is not required for all submissions).

Critical Elements	Exemplary (100%)	Proficient (85%)	Needs Improvement (55%)	Not Evident (0%)	Value
Executive Summary	Meets "Proficient" criteria and executive summary is of professional quality and situates the reader effectively into the report without unnecessary detail	Clearly articulates the general purpose, subject organization, scope, and premise of the report	Articulates the general purpose, subject organization, scope, and premise of the report, but with gaps in clarity or detail	Does not articulate the general purpose, subject organization, scope, and premise of the report	7
Organizational Background	Meets "Proficient" criteria and uses professional language to establish expertise in the focus of the report	Clearly describes the organization, background, and reasons for information security framework consultation	Describes the organization, background, and reason for information security framework consultation, but with gaps in detail or clarity necessary to set the stage for an organization analysis	Does not describe the organization, background, and reason for information security framework consultation	7
Scope	Meets "Proficient" criteria and uses professional language to establish expertise in the areas within the scope of the analysis	Clearly and accurately identifies the scope of the information security framework analysis	Identifies the scope of the analysis, but with gaps in clarity or accuracy	Does not identify the scope of the analysis	7
Approach	Meets "Proficient" criteria and approach taken shows keen insight into the nuances of balancing security with business needs	Details and defends an appropriate approach for determining the security posture of the organization	Details and defends the approach taken, but approach is not appropriate for determining the security posture	Does not detail and defend the approach taken	7
Security Posture	Meets "Proficient" criteria and determinations show keen insight into the factors that create acceptable levels of risk in organizations	Accurately determines and explains the organization's security posture and acceptable risk	Inaccurately determines and explains the organization's security posture and acceptable risk	Does not determine or explain the organization's security posture and acceptable risk	7
Policy Errors and Gaps	Meets "Proficient" criteria and the detail and focus of the analysis shows keen insight into the potential threats and risks posed by policy errors	Accurately details policy errors and gaps based on analysis of the organization's policy materials and framework	Details policy errors and gaps, but identification of errors and gaps is not accurate or is incomplete	Does not detail policy errors and gaps	7

Comparison Analysis	Meets "Proficient" criteria and comparison results in a thorough, detailed, and comprehensive identification of coverage gaps	Compares the results of analysis with ISO standards to correctly identify gaps in policy coverage	Compares the results of analysis with ISO standards, but incorrectly identify gaps in policy coverage	Does not compare the results of analysis with ISO standards	7
Technology Analysis	Meets "Proficient" criteria shows keen insight into the nuanced benefits and risks posed by the use of technology for storing, creating, sharing, or protecting information	Critically evaluates the use of technology to determine logical gaps in controls or guidelines	Evaluates the use of technology, but does not logically determine gaps in controls or guidelines	Does not evaluate the use of technology to determine gaps	7
Findings	Meets "Proficient" criteria and shows keen insight into the nuances of information security systems	Accurately assesses the extent to which the organizational information security system is deficient or ineffective	Assesses the organizational information security system, but lacks accuracy or detail regarding the extent to which the system is deficient or ineffective	Does not assess the organizational information security system	7
Policies	Meets "Proficient" criteria and proposals show keen insight into fundamental security principles and how these principles can be applied to address policy gaps	Proposes new policies or amendments that would logically cover gaps identified during analysis	Proposes new policies or amendments, but not all proposals would logically cover identified gaps	Does not propose new policies or amendments	7
Defense	Meets "Proficient" criteria and defense is articulated in terms or real-world examples that show keen insight into policy's needs	Logically defends policy proposals with examples and provides supporting information from the analysis or external sources	Defends policy proposals, but with gaps in logic or detail, or lacks supporting information or examples	Does not defend policy proposals	7
Controls	Meets "Proficient" criteria and suggestions show a keen insight into the technological and control needs of the organization	Suggests reasonable and useful controls, guidelines, and principles for integration into the organization's information security system	Suggests controls, guidelines, and principles for integration into the organization's information security system, but not all suggestions are reasonable or would be useful for the organization	Does not suggest controls, guidelines, or principles for integration into the organization's information security system	7
Implementation Plan	Meets "Proficient" criteria and details of the plan show direct alignment of policy implementation to ISO standards without gaps or lapses in coverage	Proposes a reasonable implementation plan that would ensure adherence to ISO security standards	Proposes an implementation plan that is not reasonable, or would not ensure adherence to ISO standards	Does not propose an implementation plan	7

Southern New Hampshire University

Policy Life Cycle	Meets "Proficient" criteria and claims show keen insight into the long-term requirements of security policies	Makes logical and accurate claims about maintenance needs of the policies in terms of the policy life cycle	Makes illogical or inaccurate claims about the needs of the policies in terms of the policy life cycle	Does not make claims about the maintenance needs of the policies in terms of the policy life cycle	7
Articulation of Response	Submission is free of errors related to citations, grammar, spelling, syntax, and organization and is presented in a professional and easy-to-read format	Submission has no major errors related to citations, grammar, spelling, syntax, or organization	Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas	2
				Earned Total	**100%**

Rubric Annotations

Term	Context for Instructor/Definition/Explanation
Keen insight	Shows an acute or strong understanding, awareness, or acumen of the discipline or areas within the discipline that could servee as intuition or guidance to best practices or successful solutions to issues
Nuances	Subtle distinctions, variations, layers, or facets for consideration
Long-term requirements	Considers the varying aspects of policy maintenance that must be considered, perhaps drawing in specific consideration from the industry or organization or type of security system in place. Submission may also consider aspect(s) not often looked upon in consideration of policy maintenance, such as business and financial decisions, minor updates to software, or even changing network areas