Failures in Design and Security Principles Scoring Guide

Due Date: End of Unit 5.
Percentage of Course Grade: 8%.

CRITERIA	NON-PERFORMANCE	BASIC	PROFICIENT	DISTINGUISHED
Evaluate how the security principles have been implemented within a particular organization. 20%	Does not evaluate how the security principles have been implemented within a particular organization.	Evaluates partially or at a high level how the security principles have been implemented within a particular organization.	Evaluates how the security principles have been implemented within a particular organization.	Evaluates how the security principles have been implemented within a particular organization and provides support for the position.
Analyze common security failures that exist within a particular organization. 20%	Does not analyze common security failures that exist within a particular organization.	Analyzes partially or at a high level common security failures that exist within a particular organization.	Analyzes common security failures that exist within a particular organization.	Analyze common security failures that exist within a particular organization and provides support for the position.
Identify specific design principles that have been violated within this particular organization. 20%	Does not identify specific design principles that have been violated within this particular organization.	Identifies partially or at a high level specific design principles that have been violated within this particular organization.	Identifies specific design principles that have been violated within this particular organization.	Identifies specific design principles that have been violated within this particular organization and provides support for the choices.
Explore the optimal means by which information security professionals can communicate potential areas of vulnerability to organizational executives. 30%	Does not explore the optimal means by which information security professionals can communicate potential areas of vulnerability to organizational executives.	Explores partially or at a high level the optimal means by which information security professionals can communicate potential areas of vulnerability to organizational executives.	Explores the optimal means by which information security professionals can communicate potential areas of vulnerability to organizational executives.	Explores the optimal means by which information security professionals can communicate potential areas of vulnerability to organizational executives and provides support for the position.
Exhibit proficiency in writing, critical thinking, and research topic areas in IT security fundamentals. 10%	Does not exhibit proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.	Exhibits a low level of proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.	Exhibits proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.	Exhibits a high level of proficiency in writing, critical thinking, and research topic areas in IT security fundamentals.