Project: SwiftTech Report

Submission Phase

Success Criteria	Specifications
Uploaded a presentation file for review.	The presentation contains 10 total pages. The first 5 pages are project content provided to the student to assist in completion of the project. The final 5 pages contain student content created for this project. Page 6 will contain an explanatory paragraph related to the security posture of a fictional organization. Page 7 will contain a list of 2 or 3 security standards that the student used in preparing the remaining project content. Page 8 and page 9 (optional) will contain statements about risks / control objectives made on page 2 of this presentation and whether the statements align with controls objectives the student selected on Page 7. Page 10 will include a list of 3 statements or short paragraphs depicting a process for assessing controls necessary to meet certain security control objectives.
The student has uploaded a spreadsheet for review.	The spreadsheet should contain two tabs. The primary tab contains the students risk assessment of security control objectives. The second tab is cell data provided to the student in order to complete the project.
The student has uploaded a document file for review.	The document is an Information security policy for a fictional organization modified to include security control objectives identified throughout the remainder of this project.

Security Posture

Success Criteria	Specifications
Make a determination as to the organization's likely risk posture.	Makes a correct determinative statement about the organizations likely risk posture.
Recognize unique organizational factors that influence risk posture and decision-making.	Cites specific information from the fictional company's description to support their risk posture decision. For example: The organization is likely Risk Accepting because their success hinges on the ability to innovate and fail fast.

Relevant Frameworks

Success Criteria	Specifications
List security / security control frameworks.	Must list two or three valid security control or risk frameworks.

Success Criteria	Specifications
Select relevant frameworks based on GRC goals.	Selected frameworks relevant to the organization based on information provided to the student related to the organization's overall goals.

Audit Against Frameworks

Success Criteria	Specifications
Create a list of controls and control assessments.	For every control described on page 2 of the provided presentation document, create a list item and an assessment of the control. That list should be reflected on pages 8 and 9 (optional) in the presentation document.
Align control assessment statements with selected control frameworks.	Selected the correct frameworks and has provided direction to incorporate guidance provided in the sample MSA. Assessments of control statements should come from 1 of the 3 relevant frameworks or from the MSA.

Risk Assessment

Success Criteria	Specifications
Complete provided risk assessment template.	Provided answers in each cell of the provided risk assessment spreadsheet.
Align risk statements with the provided controls.	Suggested controls or control statements provided in the risk assessment spreadsheet are taken directly from Page 2 of the provided presentation document. Created risk statements that might be derived from the control statements. For instance, if an organization only requires 2 character passwords, a logical risk might be that “there is a risk of password guessing” and therefore the ability for bad actors to access systems using stolen credentials.
Create reasonable assertions about levels of risk.	Assessed the likelihood and impact that the risk might actually occur. Described reasoning and provided an overall risk score (likelihood x impact). Risk score reasoning should approximately align to the assessed likelihood and impact scores. If, for instance, you assesses the likelihood and impact of a risk as “high”, the reasoning should indicate factors that make the risk of high consequence.

Security Policy Development

Success Criteria	Specifications
Create policy sections and short statements or paragraphs for relevant compliance headings.	Create policy statements that relate to the information provided on page 2 of the presentation document. Policy sections should include:

Success Criteria	Specifications
	Data storage End-user management Network controls Vulnerability and patch management Code scanning
Create statements that are not permissive.	Each policy statement says what the organization will or shall do. Statements that include passive words like may, should, might, or can are not appropriate for most simple policy language.
Relate statements to previous work in the audit against frameworks section.	Each policy statement should clearly express what the organization will or shall do. Each section should contain statements about what the organization will do based on prior work from the audit against frameworks section (Section 4.). For instance, if you believe that passwords should expire every 90 days, you should say that "passwords shall expire every 90 days".

Governance

Success Criteria	Specifications
Create control assessment statements that are: 1. Capable of effectively measuring provided end-user management controls. 2. Congruent with control assessments.	1. Created three control assessment statements that pertain directly to the end-user management controls provided on slide 2 of the presentation document. 2. Each statement should create a logical mechanism (such as reporting or testing) to ensure that controls are working as expected. Each statement should also provide a time element that clearly explains how frequently the assessment mechanism should be run. 3. In Section 4, you are asked to audit existing controls against selected control frameworks. Any assessment statements should be congruent with those assessments - meaning that the measurement mechanism is performed at a specific level or time schedule. For instance, if you believe that password changes should occur every 90 days, the assessment mechanism should occur every 90 days on a schedule that would detect password changes that occur outside of the 90 day period.