D485- Cloud Security
Overview – PERFORMANCE ASSESSMENT – <mark>DGN2</mark>
CLOUD SECURITY IMPLEMENTATION PLAN AND PRESENTATION

To complete this task, you will need to do outside research beyond the Learning Resources provided. At the Master's Degree level, you will be challenged to perform research of multiple collections to draft a conclusion/response.

This Guide does not substitute your TASK Page. Be sure you have read the entire TASK REQUIREMENTS AND RUBRIC.

Tips are made available for each Task Instruction below and are not a study shortcut. You are responsible for reviewing all your learning resources.

1. Task 1 – Competencies

4114.1.1 Designs Secure Cloud Solutions

> The learner designs secure cloud solutions for data protection.

4114.1.2 Implements Security Cloud Solutions

> The learner implements secure identity and access management cloud solutions for data protection.

4114.1.3 Analyzes Risk Management Plan

> The learner analyzes a risk management plan for threat mitigation countermeasures in the cloud.

2. Task 1 – Introduction to the Rubric

- You can check your work by comparing your responses to each task prompt against the criteria of the rubric.

You must use the rubric to direct the creation of your submission because it provides detailed criteria that will be used to evaluate your work. Each requirement below may be evaluated by more than one rubric aspect. The rubric aspect titles may contain hyperlinks to relevant portions of the course.

3. Task 1 – Formatting

- Paraphrase
  - No more that 30% unoriginal work will be accepted.
    - *No more than a combined total of 30% of a submission and no more than a 10% match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly.*
- APA Format
  - APA Formatting and Style Guide
    - *You can visit the WGU Writing Center for help and/or examples of creating references and in-text citations.*
    - https://owl.english.purdue.edu/owl/resource/560/01/

Note: When using sources to support ideas and elements in a paper or project, the submission MUST include APA formatted in-text citations with a corresponding reference list for any direct quotes or paraphrasing.

4. Task 1 – Task Technical Details

*You will use the provided content, Supporting Documents & Lab to develop your responses, be sure to take the time to read the Introduction, Scenario, Requirements, Web Links Supporting Documents and Rubric. *In the Lab Environment (Under the Resources Tab) Resource Groups, Key Vaults and Backup Vaults and Users are listed there.*

In your lab instance, you will be provided accounts on the right-hand side that correspond to the specific job roles. Use **only** those accounts to complete your task. You may see other accounts or groups in the lab, but those should not be used.

EXECUTIVE SUMMARY

A.   Provide an executive summary of the company's current security environment based on the business requirements given in the "Company Overview and Requirements" document.

You want to discuss the current state of SWBTL LLC's security environment and business requirements.

> *TIP: Refer to the Task Introduction and Scenario on your Task Page and the Company Overview and Requirements.docx in the Supporting Documents on your Task Page.*
> *Review the current Azure configuration in the Lab Environment*

RUBRIC - COMPETENT
An executive summary of the company's current security environment is provided and is in alignment with the business requirements given in the "Company Overview and Requirements" document.

PROPOSED COURSE OF ACTION

B.   Describe a proposed course of action for a secure Azure cloud solution for the company, based on the given scenario, and include the following in your description:

• identification of the service model
• applicable regulatory compliance directives
• security <u>benefits and challenges</u> of transitioning to this service model

*You want to discuss your proposed course of action to secure the Azure environment based on the company <u>Scenario and Company Overview and Requirements.docx</u>. **Be sure to address all 3 points listed.***

> *TIP: Refer to Section 1 of your Learning Content – Design Secure Cloud Solutions; to develop an understanding of Shared Responsibility, NIST Security Standards, and Architecture Concepts.*

RUBRIC - COMPETENT

The submission describes a proposed course of action for a secure Azure cloud solution for the company. The description includes *all* 3 requirements and is in alignment with the given scenario.

RBAC RECOMMENDATIONS & RBAC CONFIGURATION
C.   Analyze the current state of role-based access controls in the cloud lab environment for **the marketing, accounting, and IT resource groups.**

1. Discuss **three** recommendations for role-based access controls that can be configured in alignment with the principle of least privilege based on the business requirements in the given scenario.
Log into the Lab Environment. Review the Business Requirements and the current configuration of the Azure Lab Env. You want to discuss 3 recommendations for RBAC aligned to the business requirements and observing the principle of least privilege.

> *TIP: Refer to the Supplemental Resources posted in your Course Tips for Videos and Guided Labs hosted by the WGU Library.*

2. Configure the role-based access controls in alignment with your given recommendations in part C1 and provide **a screenshot for *each* of the updated configurations. The screenshots must be clear and show the full view of your screen, including the date and time.**
Log into the Lab Environment. Review the Business Requirements and the current configuration of the Azure Lab. Capture screen shots and articulate those screen shots showing the implementation of your recommendations from C1.

> *TIP: Refer to the Company Overview and Requirements.docx*
> *Review the state of the Lab and the Provided Resource Groups in the Lab: Marketing-rg, Accounting-rg, IT-rg (these are listed on the right-hand side of the Lab Env under the Resource Tab).*
> *Refer to Section 2 of your Learning Content – Implement Secure Cloud Solutions; to develop an understanding of Azure Role Based Access Control, Azzure Security Principles, Azzure Resources, and*

Identity and Access Management. Refer to the Course Tips for supplemental resources and links to Guided Practice in the WGU Library.

RUBRIC - COMPETENT

C.1 The submission discusses 3 recommendations for role-based access controls that can be configured in alignment with the principle of least privilege. The recommendations are in alignment with the business requirements in the given scenario and are accurate for *each* resource group listed.

C2. The configurations of role-based access controls are correctly completed in the cloud lab environment and are in alignment with the recommendations given in part C1. Screenshots are provided for *each* updated configuration and are clear and show the full view of the screen, including the date and time.

D: ENCRYPTION IMPLEMENTATION & ENCRYPTION RECOMMENDATIONS

D. Analyze the existing Azure Key Vaults in the cloud lab environment focusing on encrypting data in transit and data at rest for the marketing, accounting, and IT resource groups.

1. Implement **two** best practices for Azure Key Vaults applicable to the resource groups listed and in alignment with the given scenario, providing screenshots of your updated access policies for *each* group. The **screenshots must be clear and show the full view of your screen, including the date and time**.

Log into the Lab Environment. Review the Business Requirements and the current configuration of the Key Vaults. Implement 2 best practices applicable to the resource groups; take screen captures and articulate your implementation.

2. Explain **two** recommendations for how the key vaults can be used to encrypt *both* data at rest and data in transit.

You want to discuss 2 recommendations for data at rest and 2 recommendations for data in transit. Be sure your recommendations are applicable to the scenario; do not generalize.

> *TIP: Refer to the Company Overview and Requirements.docx*
> *Review the state of the Lab and the Key Vaults.*
> *Refer to Section 2 of your Learning Content – Implement Secure Cloud Solutions; to develop an understanding of Encryption, Azure Key Vaults, and Encryption Compliance. Refer to the Course Tips for supplemental resources and links to Guided Practice in the WGU Library.*

RUBRIC - COMPETENT

D1. 2 best practices for Azure Key Vaults are implemented in the lab environment. The practices implemented are applicable to the resource groups listed and are in alignment with the given scenario. Screenshots are provided of the updated access policies for *each* group and are clear and show the full view of the screen, including the date and time.

D2. The submission accurately explains 2 recommendations for how the key vaults can be used to encrypt *both* data at rest and data in transit.

FILE BACKUP CONFIGURATION & FILE BACKUP EXPLANATION

E. Analyze the current state of file backups in the cloud lab environment for the company.

1. Configure **two** settings for file backups that are in alignment with the given scenario, providing screenshots of your updated configurations. The **screenshots must be clear and show the full view of your screen, including the date and time.**

Log into the Lab Environment. Review the Business Requirements and the current configuration of the Back-Up Vault. Configure 2 settings to modify the policy in alignment with SWBTL's Business Requirements, take screen captures and articulate your implementation.

2. Explain how the updated configurations from part E1 support the business requirements.

Discuss how your policy modifications support SWBTL's Business Requirements.

> *TIP: Refer to the Company Overview and Requirements.docx*
> *Review the state of the Lab and the Back-Up Vault.*
> *Refer to Section 2 of your Learning Content – Implement Secure Cloud Solutions; to develop an understanding of Azure Back Up Policies (RTO/RPO requirements), Disaster Recovery, and Data Policies. Refer to the Course Tips for supplemental resources and links to Guided Practice in the WGU Library.*

RUBRIC - COMPETENT
E1. The configurations of 2 settings for file backups are correctly completed in the cloud lab environment and are in alignment with the given scenario. Screenshots are provided for *each* updated configuration and are clear and show the full view of the screen, including the date and time.

E2. The submission accurately explains how the updated configurations from part E1 support the business requirements.

DIVISION OF RESPONSIBILITIES, RISKS and COMPLIANCE RECOMMENDATIONS

F. Describe the division of security responsibilities between the company and the cloud service provider (Azure), including shared responsibilities if any, for the cloud service model you selected in part B.
You want to discuss the division of security responsibilities and shared responsibilities between SWBTL and the cloud service provider for the cloud service model you discussed in Section B.

1. Discuss three risks assumed by the company for the cloud service model based on the shared responsibilities identified in part F, and include in your discussion the level of impact each risk may have on the company's use of cloud computing resources.

You want to discuss 3 risks and their impact (for each risk) assumed by SWBTL as it relates to shared responsibilities; for the cloud service model you discussed.

2. Explain three recommendations to ensure compliance with the company's cloud security posture, and include a justification based on industry best practices for each recommendation.

You want to discuss 3 recommendations to ensure compliance. Be sure your recommendations are applicable to your findings; do not generalize.

> *TIP: Refer to the Company Overview and Requirements.docx in the Supporting Documents on your Task Page which details the Regulations SWBTL must comply with.*
> *Refer to Section 1 of your Learning Content – Design Secure Cloud Solutions; to develop an understanding of Clous Deployment Models, Cloud Migration Strategies, Solutions for Compute, and Industry Controls.*
> *Refer to Section 3 of your Learning Content – Analyze Risk Management Plan to develop an understanding of Handling Compliance and Regulation, Reduce Variability and Applying Controls.*
> *Include in-text citations and references where needed.*

RUBRIC - COMPETENT
F. The submission accurately describes the division of security responsibilities between the company and the cloud service provider, including shared responsibilities if any, for the cloud service model selected in part B. The description is in alignment with the given scenario and the cloud service model.

F1. The submission discusses 3 risks assumed by the company for the cloud service model based on the shared responsibilities identified in part F and includes the level of impact each risk may have on the company's use of cloud computing resources.

F2. The submission explains 3 relevant recommendations to ensure compliance with the company's cloud security posture and includes a justification based on industry best practices for each recommendation.

POTENTIAL THREATS
G.   Explain **three** threats that have the potential to impact the company's updated cloud solution, and include in the explanation the threat mitigation countermeasures that could be used to minimize the impact of *each* threat.
You want to discuss 3 threats that could impact SWBTL LLC's updated cloud configuration (include how you believe these threats impact SWBTL). Also include the countermeasures you recommend to mitigate each of these threats you discuss.

> *TIP: Refer to Section 3 of your Learning Content – Analyze Risk Management Plan; to develop an understanding of Threat Actors, Mitigation Countermeasures and Analyzing Risk.*
> *Include in-text citations and references where needed.*

RUBRIC - COMPETENT
The submission accurately explains 3 threats that have the potential to impact the company's updated cloud solution. The explanation includes relevant threat mitigation countermeasures that could be used to minimize the impact of *each* threat.

SOURCES – links to the WGU Writing Center
H. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

RUBRIC - COMPETENT
The submission includes in-text citations for sources that are properly quoted, paraphrased, or summarized and a reference list that accurately identifies the author, date, title, and source location as available.

PROFESSIONAL COMMUNICATION- links to the WGU Knowledge Center

I. Demonstrate professional communication in the content and presentation of your submission.

RUBRIC - COMPETENT
Content reflects attention to detail, is organized, and focuses on the main ideas as prescribed in the task or chosen by the candidate. Terminology is pertinent, is used correctly, and effectively conveys the intended meaning. Mechanics, usage, and grammar promote accurate interpretation and understanding.