­

**DGN2 TASK 1: Cloud Security Implementation Plan**

Tyra Austin

College of Cybersecurity, Western Governors University

May 5, 2025

**Cloud Security Implementation Plan for SWBTL LLC**

**A. Executive Summary**

SWBTL LLC is transitioning from leased data centers to the Microsoft Azure cloud environment due to rising costs, frequent service interruptions, and growing cybersecurity concerns. The company contracts with the U.S. government and handles sensitive payment information, requiring strict compliance with FISMA and PCI DSS regulations.

However, the transition has been problematic. After the lead consultant left unexpectedly, significant security gaps were discovered. Users can view files from other departments, violating the least privilege principle. IT administrators cannot verify backups, and vulnerability scans are outdated, possibly not covering Azure assets.

These issues suggest non-compliance with regulatory standards and expose SWBTL LLC to risks such as data breaches, compliance violations, and advanced persistent threats (APTs). An immediate and structured approach is required to secure the Azure environment, ensure role-based access, configure backups, and meet encryption standards across departments.

**B. Proposed Course Of Action**

To address the security concerns and meet business needs, SWBTL LLC should use **Infrastructure as a Service (IaaS)** in Microsoft Azure. This service model allows the company to provision virtual machines, storage, and networking while maintaining control over OS, middleware, and applications. IaaS is ideal for SWBTL because it offers:

* Compatibility with internal applications
* Custom backup and encryption policies
* Support for Active Directory integration

**Regulatory Compliance**

The plan will align with:

* **FISMA** – Protects government data and mandates continuous monitoring
* **PCI DSS** – Secure cardholder data with encryption, access control, and logging
* **NIST SP 800-53** – Framework for system security controls

**Security Benefits**

* **Scalability** – On-demand resources to support marketing, accounting, and IT needs
* **Isolation** – Use of Resources Groups and Key Vaults to restrict access per department
* **Backup Control** – Daily backups and snapshot retention ensure data recovery

**Challenges**

* **Misconfigurations** – Without proper setup, users may get access to other departments’ data
* **Compliance Gaps** – Failing to implement encryption and access controls may violate regulations
* **Training Needs** – IT staff must be trained on Azure policies and automation tools

**C. Role-Based Access Control**

**C1. RBAC Recommendations**

Removing Excess Role Assignments

A review of role assignments at the subscription level confirmed that Marketing, Accounting, or IT users do not have any inherited or over-permissioned roles such as Owner or Contributor. This aligns with the principle of the least privilege by ensuring departments only have access within their scoped resource groups and key vaults.

**C2. RBAC Configuration**

1. **Marketing Resource Group – Contributor Role**

The “Contributor” role was assigned only to the Marketing user group (Marketing-User and Marketing-users-group1) within the Marketing Resource Group. This ensures that only authorized Marketing team members can create and manage resources in their group without accessing other departments.

See C1 screenshots per Appendix: Step-by-step guide to Subscription Level Role Review “Removing extra/inherited roles”

1. Accounting Key Vault – Key Vault Contributor Role

The “Key Vault Contributor” role was granted to two Accounting-specific user groups in the Accounting Key Vault (Accounting, Accounting Users Group). This configuration ensures only accounting users can manage their vault's keys, secrets, and certificates.

See C1 screenshots per Appendix: Step-by-Step guide: Assign “Key Vault Contributor” to accounting Users.

1. Subscription Level Role Review – No Over-Permissioned Access

Reviewing the subscription-level role assignments confirmed that no Marketing or Accounting users have inherited roles such as Owner or Contributor. This eliminates over-permissioned access and aligns with the principle of least privilege.

See C1 screenshots per Appendix: Step-by-step guide to Subscription Level Role Review “Removing extra/inherited roles”

**D. Encryption**

**D1. Encryption Implementation**

I configured Azure Key Vault access policies for the IT, Accounting, and Marketing departments. Each department’s key vault had access restricted to only authorized users from the same department, following the principle of least privilege. Specifically, users were assigned only the necessary permissions: Get, List, Create, and update for keys and Get, List, and Set for secrets. Certificate permissions were not granted, as SWBTL LLC did not require them. These configurations prevent unauthorized access across departments and ensure secure handling of encryption materials.

See D1 screenshots per Appendix: Step-by-step guide to Encryption Implementation in Key Vaults.

**D2. Encryption Recommendations**

Azure Key Vaults support encryption for data at rest and in transit. Azure services like Storage and Virtual Machines can be integrated with Key Vault using customer-managed keys (CMKs) for data at rest. This allows the organization to control encryption, key rotation, and revocation. For data in transit, TLS/SSL certificates stored in Key Vault help secure communications between users, apps, and services. This ensures encrypted channels are used to prevent interception of sensitive information. By properly managing key and certificate assets, Azure Key Vault helps maintain regulatory compliance and enhances the company’s overall cloud security posture.

**E. Back Ups**

**E1. File Backup Configuration**

The Recovery Services Vault created a backup policy named SWBTL in Azure. The policy is configured to run daily at 7:00 PM Eastern Time, retaining instant recovery snapshots for 3 days and daily backups for 45 days. This setup aligns with the company’s recovery requirements. The policy was applied to available virtual machines and successfully assigned to Marketing VM.

See screenshots in Appendix E1. SWBTL Backup Policy – Configuration Settings

**E2. File Backup Explanation**

The SWBTL backup policy met SWBTL LLC’s business continuity and disaster recovery needs. It is scheduled to run daily at 7:00 PM Eastern Time and retains instant recovery snapshots for three days, ensuring the company meets its recovery Point Objective (RPO) of one day. Daily backup points are also retained for 45 days, supporting the Recovery Time Objective (RTO) of 36 hours. This configuration protects critical data from loss and allows for the quick restoration of virtual machines when needed. While the marketing VM was successfully assigned to the policy, the Accounting and IT VMs were not due to lab-based restrictions related to unmanaged disks. In a real-world deployment, these VMs would be recreated with managed disks to ensure full backup compatibility. This implementation ensures data resilience and supports SWBTL’s operational goals.

**F. Division of Responsibility**

In a cloud environment like Microsoft Azure, security responsibilities are shared between the cloud provider (Microsoft) and the customer (SWBTL LLC). This is known as the Shared Responsibility Model. Microsoft is responsible for securing the physical infrastructure, including hardware, network, data centers, and host operating systems.

SWBTL LLC configures and manages its own data, access controls, identity management, virtual machines, and network settings within the Azure platform. For example, implementing backup policies like SWBTL, creating key vault access policies, and assigning RBAC roles are part of the company’s duties.

Additionally, SWBTL ensures that users follow best practices for password security, multi-factor authentication (MFA), and compliance with internal security policies. Microsoft provides tools and options, but it is up to SWBTL to use them effectively.

**F1. Risks**

If SWBTL LLC fails to fulfill its cloud security responsibilities, several risks could impact business operations and data confidentiality. For example, not implementing backup policies could result in data loss during a system failure or cyberattack. Likewise, failing to configure proper role-based access controls (RBAC) may lead to unauthorized access to sensitive data, especially if employees gain excessive privileges.

Additionally, suppose encryption settings are not correctly applied through Key Vault policies. In that case, data stored in Azure may be left unprotected at rest or in transit, increasing the risk of exposure in a breach. Ultimately, these oversights could lead to compliance violations, downtime, and a loss of customer trust. It is critical that SWBTL continuously monitors its cloud security posture and follows Azure best practices to mitigate these risks.

**F2. Compliance Recommendations**

To strengthen SWBTL LLC’s cloud security posture and maintain compliance with regulatory standards like FISMA, PCI-DSS, and NIST SP 800-53, the following three recommendations should be implemented:

1. **Enable Continuous Monitoring with Azure Security Center**

SWBTL should use Microsoft Defender for Cloud to continuously assess the environment for vulnerabilities, misconfigurations, and threats. This aligns with FISMA’s requirement for ongoing risk management and helps detect and respond to threats in real time.

1. **Enforce Least Privilege with Strict RBAC Policies**

Role assignments must be reviewed regularly to prevent privilege creep. Only department-specific users should have access to their resource groups and Key Vaults. This supports NIST access control requirements and reduces the chance of accidental or malicious insider threats.

1. **Automate Backup and Key Management**

Automating daily backups and enforcing encryption using customer-managed keys in Azure Key Vault ensures data integrity and confidentiality. This aligns with PCI-DSS requirements for protecting cardholder data and meets NIST media protection and recovery guidelines.

**G. Potential Threats**

**1. Unauthorized Access (Insider Threat or External Breach)**

Improper RBAC configurations can allow users to access resources outside their department. This threat can be mitigated by applying strict least privilege access, using Azure role assignments, and requiring multi-factor authentication (MFA) to prevent compromised credentials from being misused.

2**. Data Exposure Due to Misconfigured Encryption**

Without proper use of Azure Key Vault and encryption policies, sensitive data may be exposed in storage or transit. This can be minimized by enforcing customer-managed key (CMK) encryption, enabling soft-delete and purge protection, and routinely auditing access log anomalies.

1. Data Loss from Failed Backups or Ransomware

If backup policies are misconfigured or not applied, critical data may be lost during a system failure or a ransomware attack. To counter this, daily backups should be automated using Azure Recovery Services Vault, and retention policies should be enforced to meet recovery objectives.

**References**

Chapple, M., & Seidl, M. (2023). *(ISC)² CCSP Certified Cloud Security Professional Official Study Guide* (3rd ed.). Sybex.  
<https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3375845&site=eds-live&scope=site>

Copeland, M., Soh, J., Puca, A., & Harris, M. (2020). *Microsoft Azure: Planning, Deploying, and Managing the Cloud* (2nd ed.). Springer.  
<https://wgu.percipio.com/books/3066d572-95c9-49c4-ac7d-9a3c35458b25>

Estrin, E. (2022). *Cloud Security Handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP*. Packt Publishing.  
<https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=3198558&site=eds-live&scope=site>

Microsoft. (2023). *Shared responsibility in the cloud*. Microsoft Learn.  
<https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

Microsoft. (2023). *Azure Key Vault best practices*. Microsoft Learn.  
<https://learn.microsoft.com/en-us/azure/key-vault/general/best-practices>

Microsoft. (2023). *Back up Azure VMs with Azure Backup*. Microsoft Learn.  
<https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-vms>

National Institute of Standards and Technology. (n.d.). *NIST Cybersecurity Framework (CSF)*.  
<https://www.nist.gov/cyberframework>

PCI Security Standards Council. (2022). *PCI DSS v4.0 Requirements and Security Assessment Procedures*.  
<https://www.pcisecuritystandards.org>

Western Governors University. (2025). *D485 Skillable Lab: Cloud Security Implementation Plan* [Virtual lab environment].  
https://wgu.skillable.com