­

DGN2 TASK 1: Cloud Security Implementation Plan



Damian J. Yates

Cybersecurity and Information Assurance, WGU

D485

May 30, 2025

**Cloud Security Implementation Plan**

## A. Executive Summary

SWBTL LLC, a nationwide logistics and delivery company with over 2,000 employees, has begun migrating its operations to the Microsoft Azure cloud platform. This strategic shift is driven by rising data center costs, service interruptions, and increased cybersecurity concerns stemming from its legacy leased infrastructure. The migration also aims to support regulatory compliance with FISMA and PCI DSS, strengthen business continuity, and modernize IT operations.

A comprehensive assessment of the Azure environment identified several critical configuration issues that threaten SWBTL’s compliance, operational stability, and data security. Key findings include improperly grouped virtual machines, untagged resources, missing backup policies, and a lack of scheduled recovery configurations. In addition, none of the departmental Key Vaults had defined access policies, and no virtual machines were registered for backup, placing the organization at risk of data loss and audit failure.

If left unaddressed, these misconfigurations could result in service disruption, regulatory non-compliance, or exploitation during an upcoming NIST SP 800-53 assessment. To mitigate these risks, a structured remediation plan has been developed. This plan includes isolating departmental resources, enforcing role-based access control, enabling encryption, implementing a standardized backup policy, and applying consistent tagging. These measures will align the cloud environment with SWBTL’s business requirements and ensure regulatory readiness.

## B. Proposed Course of Action

To address the critical security and compliance issues identified in SWBTL’s Azure environment, a structured remediation plan will be implemented in alignment with industry best practices and the organization’s business requirements. This phased and risk-informed approach will begin with restoring resource isolation and enforcing granular access controls. Subsequent phases will include implementing standardized backup and recovery processes and refining encryption, tagging, and monitoring mechanisms to support long-term governance.

Accounting, Marketing, and IT departments will be assigned their dedicated Azure Resource Group and Key Vault with tightly scoped access permissions (Copeland, 2020). Virtual machines and their associated network components will be relocated to the appropriate groups, and resource tagging will be standardized to enable better identification and automation (Copeland, 2020). A centralized Recovery Services Vault will enforce a new SWBTL backup policy that ensures daily backups, 45-day retention, and 3-day snapshot recovery. All virtual machines will be enrolled in this policy to meet the organization’s recovery point and time objectives.

Encryption for data at rest and in transit will be verified and enforced using Azure-native security features, with future consideration for customer-managed keys (CMKs) where applicable (Chapple & Seidl, 2023). Role-based access control (RBAC) will be implemented alongside Key Vault access policies to ensure adherence to the principle of least privilege. Microsoft Defender for Cloud and Azure Monitor will support logging, alerting, and compliance auditing. Together, these measures will reduce SWBTL’s security risk exposure, improve regulatory alignment, and ensure that the Azure cloud infrastructure remains resilient and auditable.

## C. Role-Based Access Control

Role-based access control (RBAC) is a fundamental security mechanism for managing permissions in cloud environments. It ensures that users and systems are granted only the access necessary to perform their duties, reducing the risk of privilege misuse, data leakage, or internal compromise. In the context of SWBTL’s Azure migration, RBAC is critical for enforcing departmental resource isolation, restricting access to sensitive infrastructure components, and supporting regulatory frameworks such as FISMA and NIST SP 800-53. The following subsections detail the RBAC strategy recommended for SWBTL and the specific implementation steps taken within the Azure environment.

## C1. RBAC Recommendations

To ensure secure access management and regulatory compliance, SWBTL should adopt a role-based access control (RBAC) strategy that scopes access based on job function and departmental responsibility. This approach will enforce the principle of least privilege while reducing the risk of unauthorized access across the cloud environment.

Each department, Marketing, Accounting, and IT, should have permission restricted to resources within its designated Azure Resource Group. Users from one department should not have visibility or access to resources belonging to other departments. The IT department will retain elevated permissions for cross-group oversight and operational maintenance, but these rights will be tightly controlled and auditable.

Azure Key Vault Contributor roles should only be assigned to users within each department for their respective vaults. Administrative access to critical infrastructure components, such as backup vaults or identity configurations, should be limited to a small number of IT security personnel with clearly defined responsibilities.

## C2. RBAC Configuration

RBAC will be implemented using Azure’s built-in role assignments and will be scoped at the **resource group level**.   
The following configurations are recommended:

* Assign the **Contributor** role to each department's group of users within their respective resource groups (e.g., Marketing users to Marketing-rg).
* Assign the **Key Vault Contributor** role to specific departmental users within their department’s Key Vault.
* Assign the **Backup Contributor** role to IT team members responsible for managing Recovery Services Vault operations.
* Remove any existing access assignments that cross departmental boundaries or grant excessive privileges.
* Use **Azure AD security groups** to manage user access assignments efficiently and consistently across environments.

Access auditing will be enabled via **Azure Monitor logs** to ensure all privilege escalations and permission changes are captured and reviewed regularly. Azure Policy can be used to enforce access scoping rules as the environment matures.

\*Screenshots 4 through 7 (see Appendix A) show that role assignments were applied to users and Key Vaults using Azure RBAC.

## D. Encryption

Encryption is a critical control for maintaining the confidentiality and integrity of sensitive data within cloud environments. In alignment with FISMA, PCI DSS, and NIST SP 800-53, SWBTL must ensure that all data, both at rest and in transit, is adequately protected using platform-native and, where necessary, customer-managed cryptographic controls. The following subsections describe the current encryption status of the Azure environment and provide recommendations to strengthen encryption compliance across all resources.

## D1. Encryption Implementation

In the current Azure environment, encryption is supported by default for many services, but it has not yet been validated or documented per SWBTL’s compliance requirements. Azure provides built-in encryption at rest using platform-managed keys for virtual machines, managed disks, and storage accounts. Additionally, data in transit is protected via HTTPS for most Azure-native services.

However, there is no indication that customer-managed keys (CMKs) or additional encryption policies have been configured for sensitive resources. No centralized validation process is in place to confirm encryption status across all virtual machines, storage, and databases, and no integration with Azure Key Vault for advanced key management has been established. (Copeland, 2020).

## D2. Encryption Recommendations

To meet FISMA and PCI DSS requirements, SWBTL should validate and enforce encryption for all data at rest and in transit throughout Azure. This includes:

* Ensuring that all **VM disks**, **Azure Storage**, and **SQL databases** are encrypted using **Azure-managed keys** at a minimum.
* Requiring **HTTPS endpoints** for all public-facing applications and enforcing **TLS 1.2 or higher**.
* Evaluating the use of **Customer-Managed Keys (CMKs)** stored in Azure Key Vault for sensitive workloads.
* Enabling and auditing **Storage Service Encryption (SSE)** for blob and file shares.
* Applying Azure Policy definitions to require encryption on newly deployed resources.

A centralized reporting process should be implemented using Microsoft Defender for Cloud or Azure Policy compliance dashboards to monitor encryption coverage and flag deviations continuously.

## E. Back Ups

Reliable backup and recovery procedures ensure data availability and business continuity in cloud environments. Per SWBTL’s operational goals and compliance obligations under FISMA and PCI DSS, all virtual machines must be protected by scheduled backups and long-term retention policies. The following subsections assess the current backup configuration within Azure and detail the implementation of a compliant backup strategy.

## E1. File Backup Configuration

The current Azure configuration includes a single Recovery Services Vault named Backup-Vault in the IT-rg resource group. However, no virtual machines are registered for backup, and the required SWBTL backup policy has not been created. Existing policies do not meet SWBTL’s business continuity requirements, with retention periods set to 30 days instead of 45 days and instant recovery snapshots retained for only 2 days instead of 3 (Copeland, 2020). Additionally, backups are scheduled at off-hours (e.g., 3–5 AM UTC), which do not align with the specified daily backup time of 7:00 PM Eastern Time.

There is also no evidence that backup verification procedures are being conducted or alerts configured for backup success or failure. This violates SWBTL’s recovery time objective (RTO) and recovery point objective (RPO) requirements. (Copeland, 2020).

\* Screenshot 8 (See Appendix A)confirms the creation of the SWBTL policy

## E2. File Backup Explanation

A new backup policy named SWBTL will be created and applied to all virtual machines. This policy will:

* Schedule **daily backups at 00:00 UTC (7:00 PM ET)**
* Retain **instant recovery snapshots for 3 days**
* Retain **daily backups for 45 days**
* Apply to all VMs using a centralized **Recovery Services Vault**

The IT department will be responsible for configuring, verifying, and maintaining these backups. Alerts will be enabled to notify IT staff of backup job success or failure. Azure Monitor and Microsoft Defender for Cloud will track backup health and audit restore capabilities.

This configuration ensures compliance with SWBTL’s internal policies and FISMA and PCI DSS requirements for business continuity and disaster recovery.

## F. Division of Responsibility

In the updated Azure cloud environment, responsibilities will be divided between the IT department, departmental users (Accounting, Marketing), and Microsoft as the cloud service provider. SWBTL will follow a **shared responsibility model**, where Microsoft is responsible for the security *of* the cloud (e.g., physical infrastructure, underlying hypervisors). At the same time, SWBTL is responsible for security *in* the cloud (e.g., identity management, access control, backup, and configuration) (Estrin, 2022).

* The **IT department** will oversee cross-departmental operations such as backup configuration, monitoring, logging, encryption policy validation, and enforcing compliance controls.
* **Departmental users** will be limited to managing their resources within their assigned Azure Resource Groups and Key Vaults, ensuring minimal risk of privilege overreach.
* **Azure administrators** will configure and monitor RBAC, tag enforcement, backup schedules, and encryption settings using Azure Policy, Defender for Cloud, and Azure Monitor.

All activities will be documented, audited, and reviewed regularly to ensure continued alignment with SWBTL’s cloud security standards.

## F1. Risks

The current configuration poses several significant risks that must be mitigated to ensure operational resilience and regulatory compliance:

* **Data Loss Risk**: No virtual machines are currently enrolled in backup, which could result in permanent data loss during outages or attacks.
* **Access Control Failures**: Key Vaults are unprotected, and cross-departmental resources reside in the wrong RGs, which increases the risk of unauthorized access.
* **Compliance Risk**: Misaligned retention policies, missing encryption validations, and lack of backup testing jeopardize compliance with FISMA, PCI DSS, and the upcoming NIST SP 800-53 audit.
* **Visibility and Ownership Confusion**: The absence of tagging prevents precise ownership tracking and impedes effective cost, security, and operational management.

\* **Before remediation, multiple resources were incorrectly grouped (see Appendix A, Screenshot 1 ), with misaligned virtual machines and Key Vaults (Appendix A, Screenshots 2 and 3).**

## F2. Compliance Recommendations

To mitigate the identified risks and ensure alignment with regulatory and organizational standards, SWBTL should adopt strategic cloud governance practices grounded in automation, visibility, and accountability.

First, SWBTL should implement Azure Policy to automatically enforce key security configurations such as encryption, resource tagging, and RBAC scoping. By codifying these standards as policy definitions, the organization can ensure that all current and future deployments conform to security baselines without relying on manual intervention. For example, policies can be assigned at the subscription level to block the creation of untagged resources or deny access to storage accounts without encryption enabled.

Next, enabling Microsoft Defender for Cloud will provide SWBTL with a unified view of its security posture. This platform offers continuous assessment of resource configurations, generates security recommendations, and maps compliance to frameworks such as NIST SP 800-53, PCI DSS, and FISMA. Defender for Cloud also integrates with Azure Monitor and Sentinel to raise alerts on anomalous activities, failed logins, and configuration drift.

In addition to automated tooling, SWBTL should conduct monthly internal compliance reviews. These reviews will leverage Azure Advisor insights and prebuilt regulatory compliance initiatives to identify deviations, measure progress, and assess gaps. This cadence ensures timely remediation and compliance does not lapse due to environmental or policy changes.

Quarterly restore drills should be performed to validate SWBTL’s backup and disaster recovery capabilities. These tests will confirm that backups are restorable within the defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). These exercises not only confirm technical readiness but also improve the incident response maturity of IT staff.

Finally, all administrative activities—including policy changes, backup verifications, and access modifications—should be recorded in a centralized operations log. This log serves as a single source of truth for internal audits and provides defensible documentation in the event of a regulatory review or incident investigation.

Together, these measures will ensure that SWBTL maintains a defensible security posture, meets federal contract requirements, and builds a resilient, auditable Azure environment that aligns with modern cybersecurity frameworks.

\* **Screenshot 9 and Screenshot 10 show that departmental tags were successfully applied to all virtual machines and Key Vaults.**

## G. Potential Threats

SWBTL’s current Azure configuration exposes the organization to multiple security and operational threats that could significantly disrupt business operations or jeopardize federal contracts. These threats are primarily the result of misconfigurations, limited enforcement of security best practices, and incomplete implementation of cloud-native controls.

1. **Insider Threats and Unauthorized Access:**  
   Virtual machines and sensitive resources were initially grouped incorrectly in a centralized resource group, increasing the risk that users could inadvertently or maliciously access systems outside their department (Chapple, 2023). This violates the least privilege principle and increases the likelihood of internal data breaches.
2. **Data Loss from Unprotected Infrastructure:**  
   Before remediation, no deployed virtual machines were protected by a backup policy, meaning a single outage or cyberattack could have resulted in irreversible data loss. Backup schedules and retention settings also failed to meet business continuity requirements.
3. **Compliance Violations:**  
   As SWBTL is subject to FISMA, PCI DSS, and an upcoming NIST SP 800-53 audit, the absence of enforced encryption, access control policies, tagging, and tested recovery procedures posed significant compliance risks (National Institute of Standards and Technology, n.d.).
4. **Limited Threat Visibility:**  
   Without centralized monitoring, logging, or alerting, there is little insight into misconfigurations, failed backups, or unauthorized access attempts. This lack of visibility makes detecting and responding to security incidents significantly more difficult (Estrin, 2022).
5. **Elevated Risk from Shadow IT and Mismanagement:**  
   The absence of consistent resource tagging and policy enforcement increases the likelihood of “orphaned” or unmanaged resources. These gaps introduce operational inefficiencies, potential security vulnerabilities, and cost overruns.

Addressing these potential threats required immediate attention to access management, encryption enforcement, backup configuration, and compliance oversight. With the implemented remediation plan, SWBTL has significantly reduced its risk exposure and improved the security and resilience of its Azure environment.

## Conclusion

SWBTL’s Azure environment assessment revealed several misconfigurations that posed significant operational, security, and compliance risks. Through structured remediation, virtual machines and Key Vaults were properly isolated by department, access controls were tightened using Azure RBAC, and a standardized backup policy was implemented to meet the organization’s RPO and RTO requirements. Departmental tagging and logging recommendations were introduced to strengthen governance and support audit readiness. With these changes, SWBTL’s cloud infrastructure aligns with FISMA, PCI DSS, and NIST SP 800-53 standards and is positioned to support secure and scalable operations.

## References

Chapple, M. &. (2023). *(ISC)² CCSP Certified Cloud Security Professional Official Study Guide (3rd ed.).* Sybex.

Copeland, M. S. (2020). *Microsoft Azure: Planning, Deploying, and Managing the Cloud (2nd ed.).* Springer.

Estrin, E. (2022). *Cloud Security Handbook: Find out how to effectively secure cloud environments using AWS, Azure, and GCP.* Packt Publishing.

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

## Appendix A

|  |  |  |
| --- | --- | --- |
| **Screenshot #** | **Description** | **Filename** |
| 1 | Initial resource group structure | 01-initial-resource-groups.png |
| 2 | VM moved to the correct department resource group | 02-vm-move-accounting.png |
| 3 | Key Vaults moved to correct RGs | 03-kv-move-accounting-marketing.png |
| 4 | Role assignment for IT user on IT-rg | 04-role-it-rg.png |
| 5 | Role assignment for Marketing user on Marketing-rg | 05-role-marketing-rg.png |
| 6 | Role assignment for Accounting user on Accounting-rg | 06-role-accounting-rg.png |
| 7 | RBAC on Key Vault via Azure Role Assignment | 07-acct-keyvault-rbac-access.png 07-it-keyvault-rbac-access.png 07-mkt-keyvault-rbac-access.png |
| 8 | Backup policy named SWBTL created | 08-backup-policy-swbtl.png |
| 9 | VM protected using SWBTL backup policy | 09-backup-protection-enabled.png |
| 10 | Tags applied to accounting-vm | 10-tag-accounting-vm.png |
| 11 | Tags applied to Key Vaults | 11-tag-keyvaults.png |

Screenshot Reference Table