Rebuilding Trust in the Cloud: Post-Incident Security Remediation and Compliance Realignment at SWBTL LLC

Elijah Olson

Western Governors University

D485 – Cloud Security

Executive Summary

Since 1977, SWBTL LLC has grown into a leader in nationwide services through the continued successful integration of technology, as it has expanded its shipping services. No stranger to implementing innovative strategies, SWBTL has embarked on a significant journey of migrating data storage from on-premises solutions to the Microsoft Azure cloud environment. This strategic move, although challenging, is crucial for the organization's future. Despite encountering issues with access control, data retention, data backup, and security validation since the migration began, the importance of this transition cannot be overstated.

Due to SWBTL supporting federal contracts and processing payment card transactions, integration of Azure cloud solutions must maintain compliance with the Federal Information Security Modernization Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS). Verifying that cloud security configurations meet regulatory requirements is paramount to the continued success of SWBTL. It ensures that systems are not left vulnerable to exploitation by advanced persistent threats or malicious actors.

Following the departure of a disgruntled employee, SWBTL finds itself lacking essential documentation for tasks previously handled by this individual, as well as cybersecurity concerns. The departure of this employee has left SWBTL vulnerable to potential security breaches, as the individual had access to critical systems and data. The purpose of the recommendations contained within this report is to provide recommendations and implementation of configuration changes to align SWBTL’s systems to comply with regulatory and business requirements. Determinations made will include the allocation of appropriate and shared responsibilities for users, identification of risks and threats, and the implementation of suitable countermeasures.

Proposed Course of Action

The organization has determined to continue providing the quality expected by its customers by embracing innovation through migration to a cloud-based environment. This commitment to quality service remains unwavering, even in the face of technological challenges. Organizational requirements for cloud service migration include control over virtual servers and operating systems, essential support for custom and legacy applications, customization of department-specific resources, custom backup and recovery management, meeting minimum compliance requirements, and integrating their current on-premises Active Directory with the Azure Active Directory service within the cloud environment. Based on the outlined needs, the recommendation is to utilize the Infrastructure as a Service (IaaS) model of cloud-based services.

IaaS is a cloud-based service that provides scalable cloud infrastructure, eliminating the need for organizations to maintain physical hardware (Microsoft). IaaS provides on-demand servers, storage, and networking capabilities virtually (Microsoft). Data centers are provided by the cloud service provider to the customer to access via a web interface or API (Microsoft). The organization only pays for resources used and has the ability to scale resources up or down based on business need (Microsoft). This solution also provides greater business continuity, as data is stored in cloud data centers with geographically dispersed locations for data backups, thereby decreasing the impact of an outage at an individual data center on the organization (Microsoft).

Given the organization's continued servicing of federal contracts it is required to comply with the Federal Risk and Authorization Management Program (FedRAMP) established by the Office of Management and Budget (OMB) with the purpose to standardize and streamline security assessment and authorization processes for cloud products and service used by any entity conducting business with the federal government ("United States Code, 2018 Edition,

Supplement 5, Title 44 - PUBLIC PRINTING and DOCUMENTS"). FedRAMP utilizes the NIST 800-145 recommendations for cloud services to assist in establishing processes and identification of criteria to make cloud products or services eligible for authorized use with systems interacting with federal government systems ("United States Code, 2018 Edition, Supplement 5, Title 44 - PUBLIC PRINTING and DOCUMENTS"). NIST 800-145 provides definitions for components involved in cloud computing (Mell and Grance). NIST800-210 creates guidance for federal government and third-party entities that conduct business with the federal government surrounding their implementation of cloud service technologies (Hu et al.).

With any technology, there are benefits and challenges to implementing the solution, and cloud technology is no exception. The first benefit of cloud implementation is centralized and scalable security controls and infrastructure (Google). Cloud data security controls focus on protecting both stored data and data in motion, both within and outside the cloud (Google). Because cloud services are elastic, the amount of protection utilized can be scaled up or down depending on organizational needs. Most cloud providers include built-in compliance standards to meet or exceed regulatory requirements, including NIST, FedRAMP, GDPR, or other applicable laws and regulations (Google).

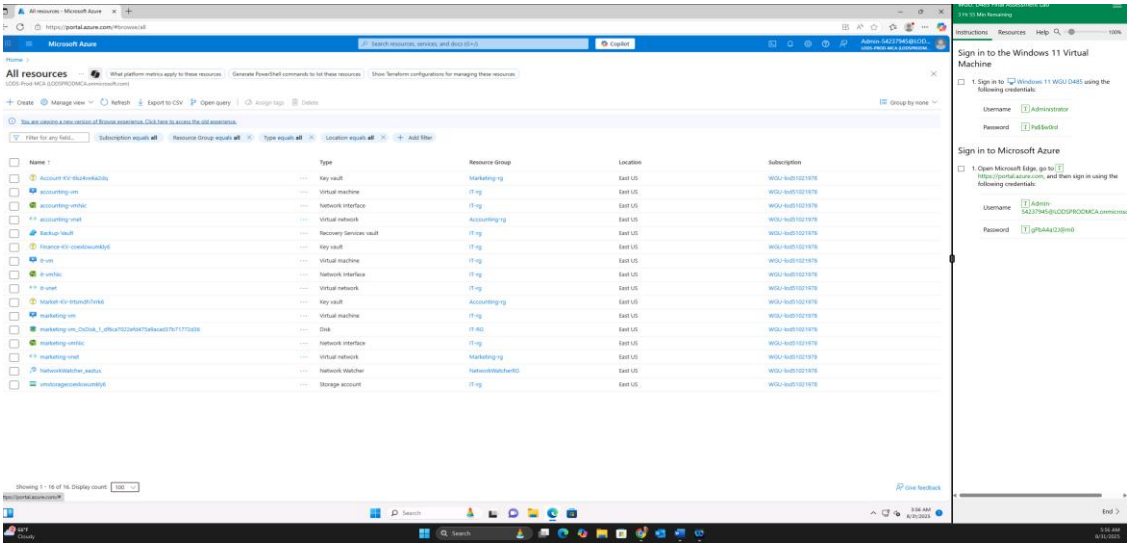
With the implementation of cloud services, the responsibilities of the organization change depending on the cloud service model selected, which is more complex than organization-based operations. One of the shared responsibility models that organizations can utilize is the IaaS previously defined. Through the migration of data to the cloud, the amount of control and visibility over the data changes, which can complicate incident response and data sovereignty, depending on where the data is being stored. Lastly, issues surrounding the correct implementation of identity and access management solutions can lead to over-provisioned

permissions. Identity and access management (IAM) involves ensuring that organizations establish rules and roles that provide the minimum amount of access necessary to perform job duties by centralizing rules and access privileges (Microsoft, “What Is Identity Access Management (IAM)? | Microsoft Security”). This can be accomplished through role-based access control (RBAC), which utilizes clearly defined job roles to group permissions needed to perform minimum job functions (Microsoft, “What Is Identity Access Management (IAM)? | Microsoft Security”).

Current Role-based Access Control Analysis

SWBTL defined business requirements for access control as correctly provisioned and configured access for each resource group, containing only the resources required for job functions within that group. Currently, the departments requiring access to cloud resources include Accounting, Marketing, and IT. The resource groups in use are correctly labeled; however, cloud resources are not assigned correctly based on business needs.

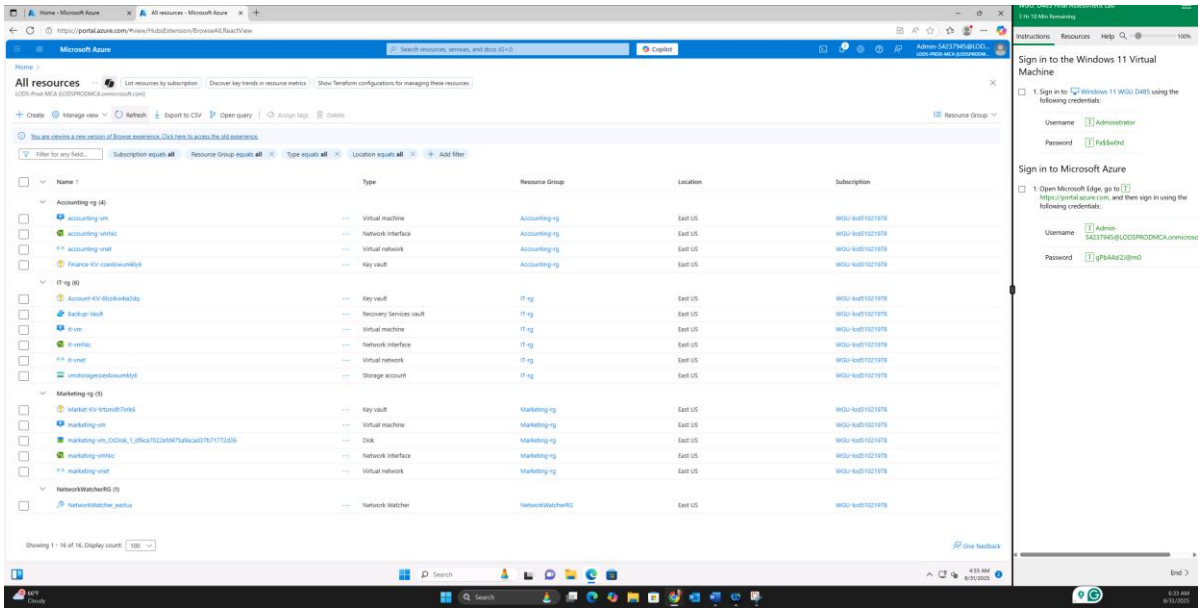
Current Configurations



Misconfigurations present include the Finance, Account, and Marketing key vaults being assigned to the wrong resource group, the Accounting virtual machines and network being assigned to the IT department. The marketing virtual machines, storage, and network are assigned to the IT department. This applies to business policies inconsistent with departmental access needs and prevents users within departments from accessing resources required for their job functions.

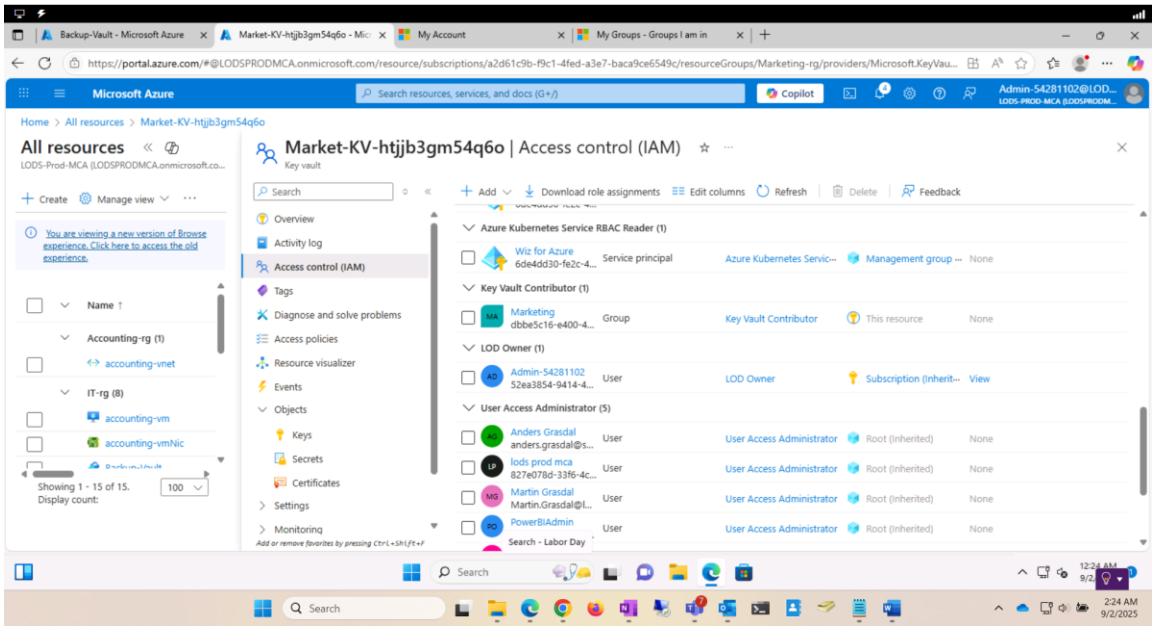
Corrected Configurations

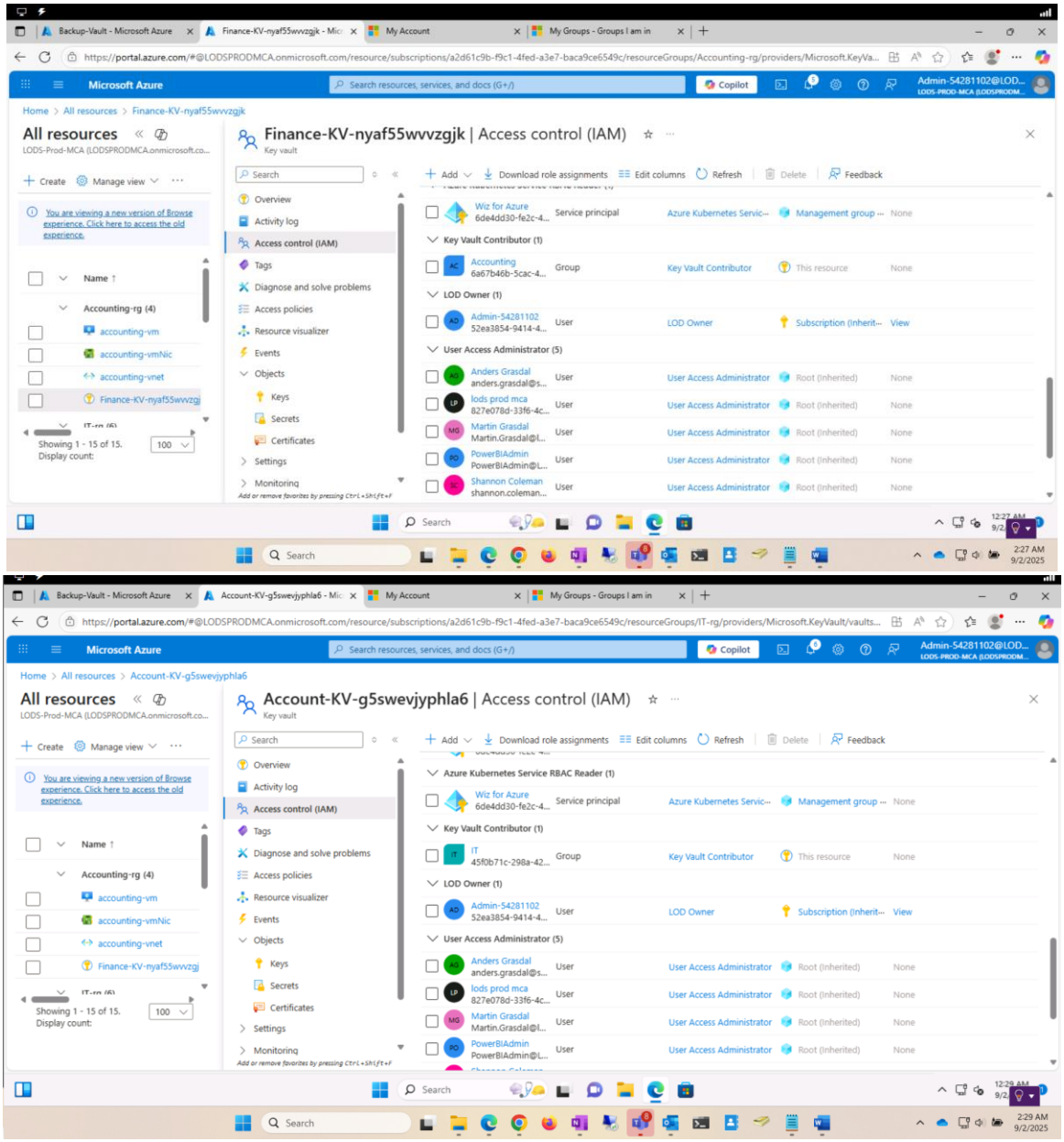
Recommendations to resolve conflicts in departmental resource allocation include reassigning the Finance key vault to the Accounting department, reassigning the Marketing key vault to the Marketing resource group, and reassigning the Accounts key vault to the IT department resource group. Next, the Accounting virtual machines and network need to be reassigned to the Accounting resource group. Marketing resources need to be reassigned to the Marketing resource group. This correctly aligns organizational resources to the applicable resource group necessary to complete job duties.



Azure Key Vaults Analysis

SWBTL organizational policies state that access to Microsoft Azure Key Vaults should be limited to departmental users only. To accomplish this, it is recommended that Role-Based Access Control (RBAC) and the principle of least privilege be implemented. This can be accomplished by establishing departmental security groups and assigning them the RBAC role of Key Vault Contributor, allowing departmental users to administer the Azure Key Vaults for their respective departments. By assigning RBAC to restrict access to Azure Key Vaults to only internal department users, the organization will have implemented the principle of least privilege. This allows individuals within the applicable department to be added to their security group, and they will inherit the necessary permissions for their job duties.





By utilizing Azure Key Vaults, encryption for data at rest is provided through the use of server-side encryption with customer-managed (Microsoft, “Server-Side Encryption of Azure Managed Disks - Azure Virtual Machines”). Server-side encryption utilizes encryption for Azure storage to protect data while meeting organizational security and regulatory compliance requirements (Microsoft, “Server-Side Encryption of Azure Managed Disks - Azure Virtual Machines”). Azure utilizes 256-bit AES encryption, which is the current industry standard and

meets FIPS 140-2 compliance (Microsoft, “Server-Side Encryption of Azure Managed Disks - Azure Virtual Machines”). Access to the stored data can only be decrypted with the appropriate encryption key, which can be customer-managed (Microsoft, “Server-Side Encryption of Azure Managed Disks - Azure Virtual Machines”).

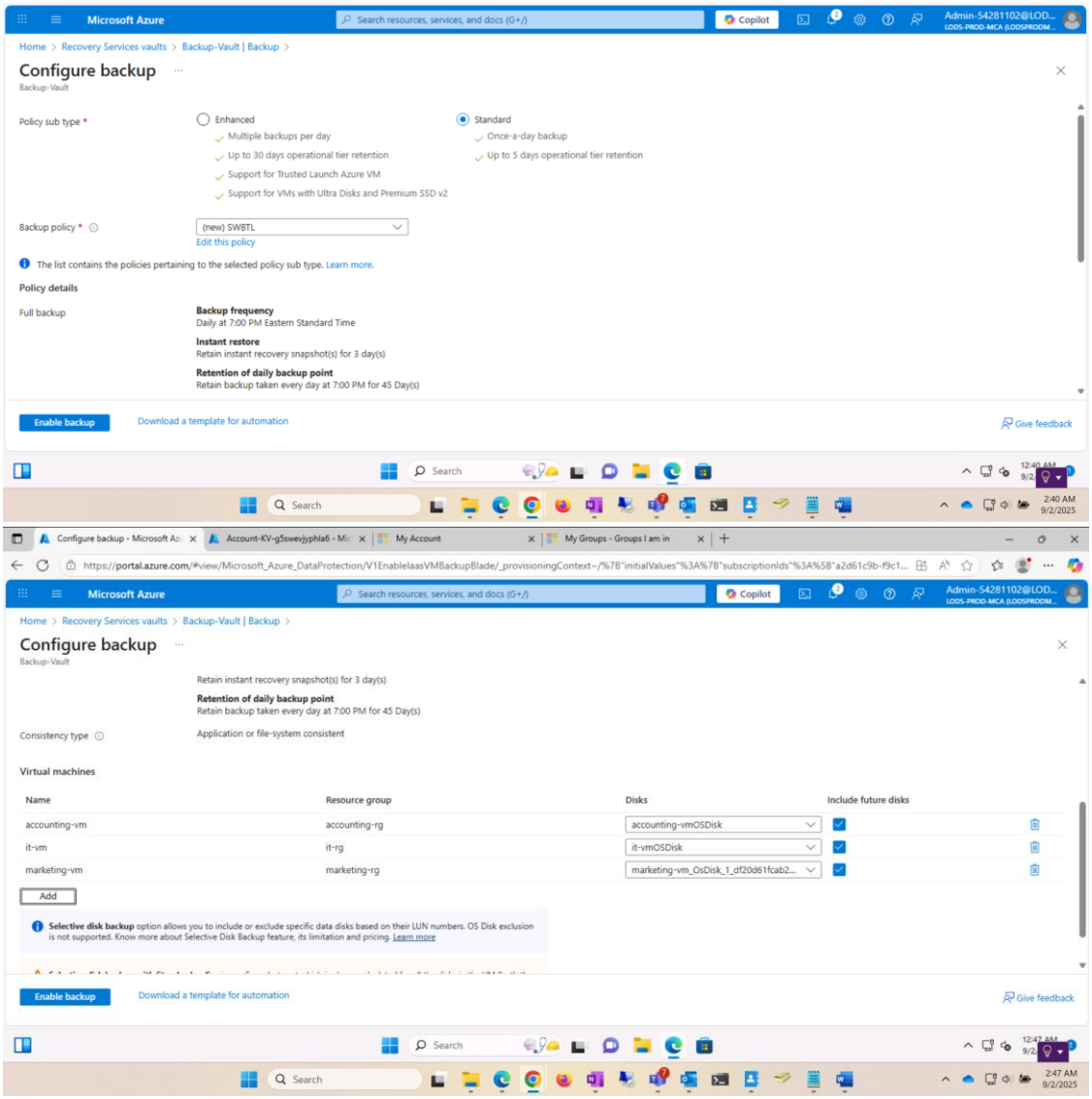
Current industry standards for encrypting data in transit utilize TLS/SSL protocols. Transport Layer Security (TLS) is an industry-standard security protocol designed to secure communications between servers and customers (Microsoft, “What Is TLS/SSL in Azure App Service? - Azure App Service”). TLS can be paired with Secure Sockets Layer (SSL) certificates to enhance the security of incoming requests to web applications (Microsoft, “What Is TLS/SSL in Azure App Service? - Azure App Service”). Azure services utilize the TLS 1.3 protocol, which provides stronger security, reduced latency, and enhanced privacy (Microsoft, “What Is TLS/SSL in Azure App Service? - Azure App Service”).

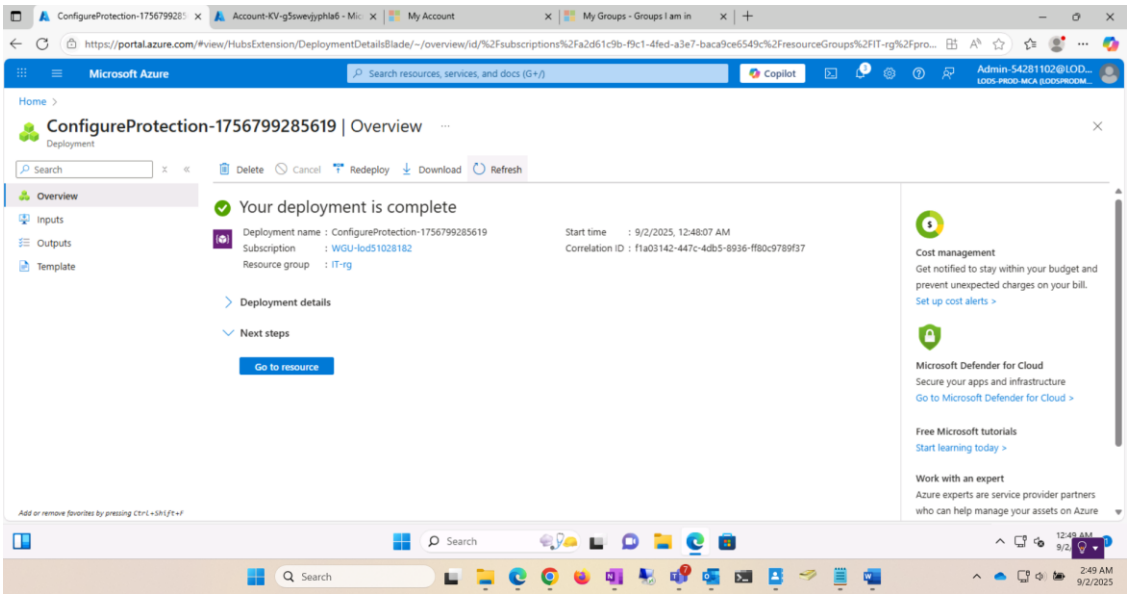
File Backup Analysis

Based on SWBTL organizational requirements all departmental backups can utilize a single recovery vault for backup storage. The organization has a recovery point objective (RPO) of 1 day which requires standard backups to be conducted daily at 7p.m. EST. This meets organizational requirements for a 36 hour recovery time objective (RTO). SWBTL requires instant recovery snapshots of systems to be maintained for 3 days and the daily backup points to be maintained for 45 days.

At the beginning of this review the centralized Backup-Vault was in existence but had no backup policies set. To ensure that organizational requirements were met, a new backup policy was created and named SWBTL. This was created as a standard backup to conduct a full backup of

organizational systems daily at 7p.m. EST with instant restore enabled and set to retain these restoration points for 3 days. The policy was set to retain all daily backups created at 7p.m. for 45 days. All department virtual machines were included within the configuration of system backups.





Security Responsibilities Division

As previously recommended, SWBTL would be best served by utilizing the IaaS shared responsibility model of cloud computing. IaaS provides computing resources by hosting and managing infrastructure within its data centers. At the same time, customers are given access to these resources with the ability to configure them for their needs, utilizing a web interface or API (Microsoft, “What Is IaaS? Infrastructure as a Service | Microsoft Azure”). IaaS reduces expenses for organizations by eliminating the need to maintain individualized data centers, while providing the elasticity to scale resources dynamically as business needs change (Microsoft, “What Is IaaS? Infrastructure as a Service | Microsoft Azure”). Additionally, IaaS provides increased reliability for organizations by removing the need to maintain and upgrade software and hardware (Microsoft, “What Is IaaS? Infrastructure as a Service | Microsoft Azure”). Lastly, organizations experienced an enhanced business continuity and disaster recovery posture due to the increased availability of resources on demand in geographically dispersed areas (Microsoft, “What Is IaaS? Infrastructure as a Service | Microsoft Azure”).

With this implementation, some identified potential risks include incorrectly configured security controls, inadequate IAM, and ineffective backup and recovery plans. Correctly configured security controls are essential for securing the use of cloud services, which includes ensuring that zero-trust security is implemented. Zero trust is a security model that defaults to denying access to resources, whether internal or external to the network. Access to resources is not granted until the user or device proves identity and authorization to the requested resources (Shaw). Other security controls that are organizational responsibility include correctly configured firewall rules and establishing storage permissions. Failure to properly configure security controls can have a significant impact on an organization's operations.

As previously identified, RBAC in the implementation of IAM ensures that the right users have the correct level of access required for their job functions without providing excessive access to resources (Microsoft, “What Is Identity Access Management (IAM)? | Microsoft Security”). RBAC is easily scalable as organizations grow, and roles can be modified as needs change. The use of IAM enables organizations to implement single sign-on, which allows users to have a single set of credentials that can be used across platforms and services to access organizational resources (Microsoft, “What Is Identity Access Management (IAM)? | Microsoft Security”). Incorrect application of IAM has the potential to impact organizational operations moderately.

Because cloud service providers are responsible for the locations where data is housed, many organizations fail to have adequate backup and recovery plans. A business continuity plan (BCP) is defined as an implemented system to allow organizations to prevent and/or recover from potential threats (Kenton). BCP involves identifying potential threats, assessing how these threats could impact operations, developing effective countermeasures and safeguards against

them, and establishing an appropriate recovery plan (Kenton). Organizations must ensure that they regularly review and test the BCP to ensure that it remains effective, including an immediate review with the transition to cloud services. Failure to establish and maintain an effective BCP could potentially have a high impact on an organization's disaster and recovery posture.

There are several ways that SWBTL can ensure compliance with its cloud security posture using continuous vulnerability management, enforcement of RBAC, and robust data retention policies. Continuous vulnerability management is defined as the process of identifying, assessing, and mitigating vulnerabilities within an organization's IT environment (SentinelOne). This can be accomplished by utilizing scanning and patching tools to automate the process (SentinelOne). Ensuring that RBAC is correctly configured, along with regular audits to verify compliance, can help mitigate the risk (Lindemulder and Kosinski). Establishing clear definitions of necessary roles, including the required resource access, ensures RBAC is successful (Lindemulder and Kosinski). Ensuring the organization has adequate data retention policies will aid in the organization's cloud security posture. First, the organization must ensure all data retention policies meet all regulatory compliance requirements ("Learn about Retention Policies & Labels to Retain or Delete"). Determining what data to back up, the frequency of data backups, and the length of time data must be retained ("Learn about Retention Policies & Labels to Retain or Delete").

Potential Threats to Cloud Solution

Potential threats to utilizing cloud solutions include potential data breaches or unauthorized access, misconfigured cloud resources, and compliance violations. Potential data breaches or unauthorized access can be caused by incorrectly configured IAM, a lack of multi-

factor authentication (MFA), and failure to encrypt data both at rest and in transit. Correctly implemented IAM solutions include properly configured RBAC to ensure that the correct individuals have the correct level of access to system resources and that encryption tools are in production (Microsoft, “What Is Identity Access Management (IAM)? | Microsoft Security”). This helps reduce data breaches and unauthorized access by ensuring that users have only the minimum access to resources required to complete their tasks, which can help prevent privilege escalation.

Misconfigured cloud resources encompass a combination of inadequately standardized resource deployments that utilize the infrastructure-as-code method. Microsoft defines this method as the DevOps methodology of defining and deploying infrastructure resources, including networks, virtual machines, and connection topologies, by defining standards for deployment that remain consistent between resources (Microsoft, “What Is Infrastructure as Code (IaC)? - Azure DevOps”). Ensuring that the initial requirements are compliant with regulations and secure, and then replicating this standard to meet unique use requirements, is less likely to introduce a vulnerability in cloud systems.

Compliance violations can occur both within and outside cloud environments, but ensuring the organization's compliance with the use of cloud systems is essential for maintaining eligibility for government contracts. This is accomplished through ensuring a thorough understanding of the organization's responsibilities regarding which regulations apply and how the division of compliance responsibilities is split between the organization and the cloud vendor. Beginning with vendors that are FedRAMP authorized ensures they meet the minimum requirements of FedRAMP. Utilizing regular internal audits and gap assessments enables the

organization to promptly identify and remediate compliance issues, ensuring continued compliance with evolving regulatory requirements.

Conclusion

SWBTL LLC grew into a leader providing nationwide services by effectively applying new technological solutions to expand its shipping services and client base. This journey has continued through the migration to cloud solutions to reduce overhead in data storage and management. With the introduction of any new technology, gaps in access control, data retention, backup, and security validation have been identified, raising concerns about maintaining compliance with regulatory requirements to ensure continued eligibility for government contracts. These concerns were exacerbated by the departure of a disgruntled employee who was largely responsible for the cloud migration. This report provides recommendations for implementing correctly configured changes to internal systems and cloud services, effectively maintaining compliance with regulatory and business requirements. These recommendations include properly configured access controls, vulnerability management, and proper data management policies.

References

Google. (n.d.). *What is cloud data security? Benefits and solutions*. Google Cloud. Retrieved August 26, 2025, from https://cloud.google.com/learn/what-is-cloud-data-security

Hu, V., Iorga, M., Bao, W., Li, A., Li, Q., & Gouglidis, A. (2020). General Access Control Guidance for Cloud Systems. *NIST*. https://doi.org/10.6028/NIST.SP.800-210

Kenton, W. (2024, November 14). *What Is a Business Continuity Plan (BCP), and How Does It Work?* Investopedia. https://www.investopedia.com/terms/b/business-continuity-planning.asp

Learn about retention policies & labels to retain or delete. (2023, August 11). Learn.microsoft.com. https://learn.microsoft.com/en-us/purview/retention?tabs=table-overriden

Lindemulder, G., & Kosinski, M. (2024, August 20). *What is role-based access control (RBAC)?* IBM. https://www.ibm.com/think/topics/rbac

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Microsoft. (2022, November 28). *What is infrastructure as code (IaC)? - Azure DevOps*. Learn.microsoft.com. https://learn.microsoft.com/en-us/devops/deliver/what-is-infrastructure-as-code

Microsoft. (2024a). *What is IaaS? Infrastructure as a Service | Microsoft Azure*. Azure.microsoft.com. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas

Microsoft. (2024b). *What is Identity Access Management (IAM)? | Microsoft Security*. Www.microsoft.com. https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam

Microsoft. (2025a, March 28). *Server-side encryption of Azure managed disks - Azure Virtual Machines*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption

Microsoft. (2025b, April 17). *What Is TLS/SSL in Azure App Service? - Azure App Service*. Microsoft.com. https://learn.microsoft.com/en-us/azure/app-service/overview-tls

SentinelOne. (2025, March 28). *What is Continuous Vulnerability Management?* SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-continuous-vulnerability-management/

Shaw, B. (2024, December 9). *What Is Cloud Security? | CrowdStrike*. Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/

United States Code, 2018 Edition, Supplement 5, Title 44 - PUBLIC PRINTING AND DOCUMENTS. (2025). Govinfo.gov. https://www.govinfo.gov/app/details/USCODE-2023-title44/USCODE-2023-title44-chap36-sec3607