Azure Cloud Compliance Assessment

Risk Mitigation & Control Mapping for NIST SP 800-53, PCI DSS, and FISMA

A. Executive Summary:

GetsIt2U is a global shipping platform contracted by the United States government (US-GOV). GetsIt2U is migrating its core departments (Marketing, Accounting, and Information Technology (IT)) to Microsoft Azure's IaaS platform to improve scalability. The initial migration has revealed three compliance gaps: (1) unauthorized user access beyond job/departmental scope, (2) unverified mission-critical backups, and (3) outdated vulnerability scanning. Addressing the findings is essential for compliance with FISMA, NIST SP 800-53 and PCI DSS. Recommended actions are to implement role-based access controls (RBACs), enforce backup verifications and scheduling, and define and maintain a vulnerability management program.

B. Business Details and Compliance Requirements:

GetsIt2U processes government-related shipments through payment card transactions. Specifically, its services involve collecting, storing, and processing sensitive data, including credit card information, of its clients and subcontractors. Therefore, GetsIt2U is required to comply with:

- PCI DSS: industry standards that apply to any entity that handles cardholder data;
- FISMA: Federal data security law that applies to entities that conduct activities on behalf of the US-GOV; and
- NIST SP 800-53: the authoritative control framework that incorporates both FISMA and PCI DSS controls, which help entities streamline their compliance efforts.

Non-compliance with these frameworks can result in regulatory fines, loss of US-GOV contracts and potential data breaches exposing sensitive cardholder data. Current cloud configurations expose the company to violations in several areas:

- Data is accessible by unauthorized users;
- Critical backup processes are not verifiable; and
- Vulnerability scanning is outdated and undefined.

To address these issues and support its compliance posture, GetsIt2U’s cloud security goals include:

- **Applying role-based access controls (RBAC)** within segmented Azure Resource Groups (RGs) for each department to ensure least privilege principle;
- **Developing and testing a backup strategy** with defined recovery point objectives (RPO) and recovery time objectives (RTO); and
- **Defining scanning boundaries and establishing a vulnerability management schedule** to detect outdated systems, misconfigurations, and missing patches.

C. Risk Summary Table:

See Appendix A. The table presents risks, its corresponding rating, and recommendations to mitigate the risks:

D. Compliance Mapping Table:

See Appendix B. This table maps identified compliance gaps to NIST SP 800-53 controls with optional PCI DSS requirements to demonstrate multi-framework readiness.

E. Secure Network Topology Design:

See Appendix C. This design represents a secure network topology by incorporating least privilege principles, including network segmentation and RBAC enforcement.

F. Technical Recommendations Summary:

It is recommended that GetsIt2U adjusts its security posture in the following ways to comply with NIST and PCI DSS:

Recommendation #1: Implement RBAC within segmented Azure Resource Groups (RGs) to enforce least privilege.

- NIST SP 800-53 AC-6(1) - (10): Enforces least privilege principles with access controls that are role-based and/or discretionary;
- PCI DSS Requirements 7.1 - 7.2: Enforces least privilege by limiting access to system components and cardholder data to only users whose roles require the access.

Recommendation #2: Implement backups of files and systems and develop a backup schedule.

- NIST SP 800-53 CP-9: Requires backups that protects the confidentiality, integrity, and availability of backup information;
- PCI DSS Requirements 12.5.1 & 12.10.1: Requires maintaining a current inventory of all system components to facilitate backup procedures.

Recommendation #3: Implement vulnerability scanning; Develop a vulnerability management schedule.

- NIST SP 800-53 RA-5(a) and (b): Requires monitoring for vulnerabilities and to periodically scan for vulnerabilities;
- PCI DSS Requirements 11.2.x: Requires vulnerability scanning of internal and external systems at least quarterly and after any significant changes in the network.

G. Conclusion:

By implementing RBACs, defining and testing a backup strategy, and establishing a vulnerability management program, GetsIt2U can significantly strengthen its Azure cloud security posture. These measures directly align with NIST SP 800-53 and PCI DSS requirements, reducing compliance risk while improving operational resilience. Addressing these gaps now will not only safeguard sensitive cardholder and government data but also position GetsIt2U for sustained compliance and long-term trust with its civilian and Federal partners.

H. References:

Microsoft. (n.d.). *Azure security and compliance documentation.* Microsoft Learn. https://learn.microsoft.com/en-us/azure/compliance/

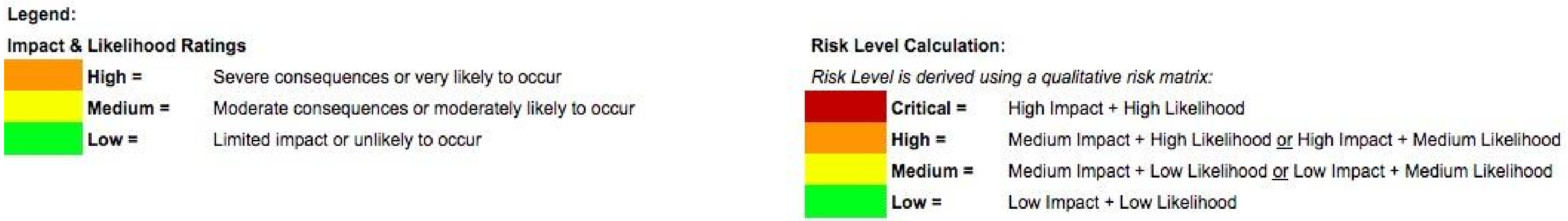
National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Revision 1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Revision 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

PCI Security Standards Council. (2022). *Payment card industry data security standard: requirements and testing procedures, version 4.0.* https://www.pcisecuritystandards.org/document_library

Appendix A: Risk Summary Table:

			RISK ASSESSMENT				
RISK ID	TOPIC	RISK DESCRIPTION	IMPACT	LIKELIHOOD	RISK LEVEL	AUDIT CONTROL	RISK RESPONSE
R-001	Access Controls	Users can access resources beyond their job roles or department boundaries, increasing the risk of data leakage or privilege misuse.	**Medium**	**High**	**High**	AC-6	Enforce access controls with least privilege principles
R-002	Disaster Recovery	No backups or backup schedule of mission-critical data, which can lead to significant consequences in the event of system failure or data loss.	**High**	**High**	**Critical**	CP-9	Conduct backups of mission-critical data; develop a backup and recovery plan and testing schedule
R-003	Vulnerability Scanning	No defined vulnerability scanning scope or cadence exists, leaving the environment exposed to unmonitored risks.	**High**	**Medium**	**High**	RA-5	Define vulnerability scanning scope; run periodic scans



Legend:

Impact & Likelihood Ratings

🟧	**High =**	Severe consequences or very likely to occur
🟨	**Medium =**	Moderate consequences or moderately likely to occur
🟩	**Low =**	Limited impact or unlikely to occur

Risk Level Calculation:

Risk Level is derived using a qualitative risk matrix:

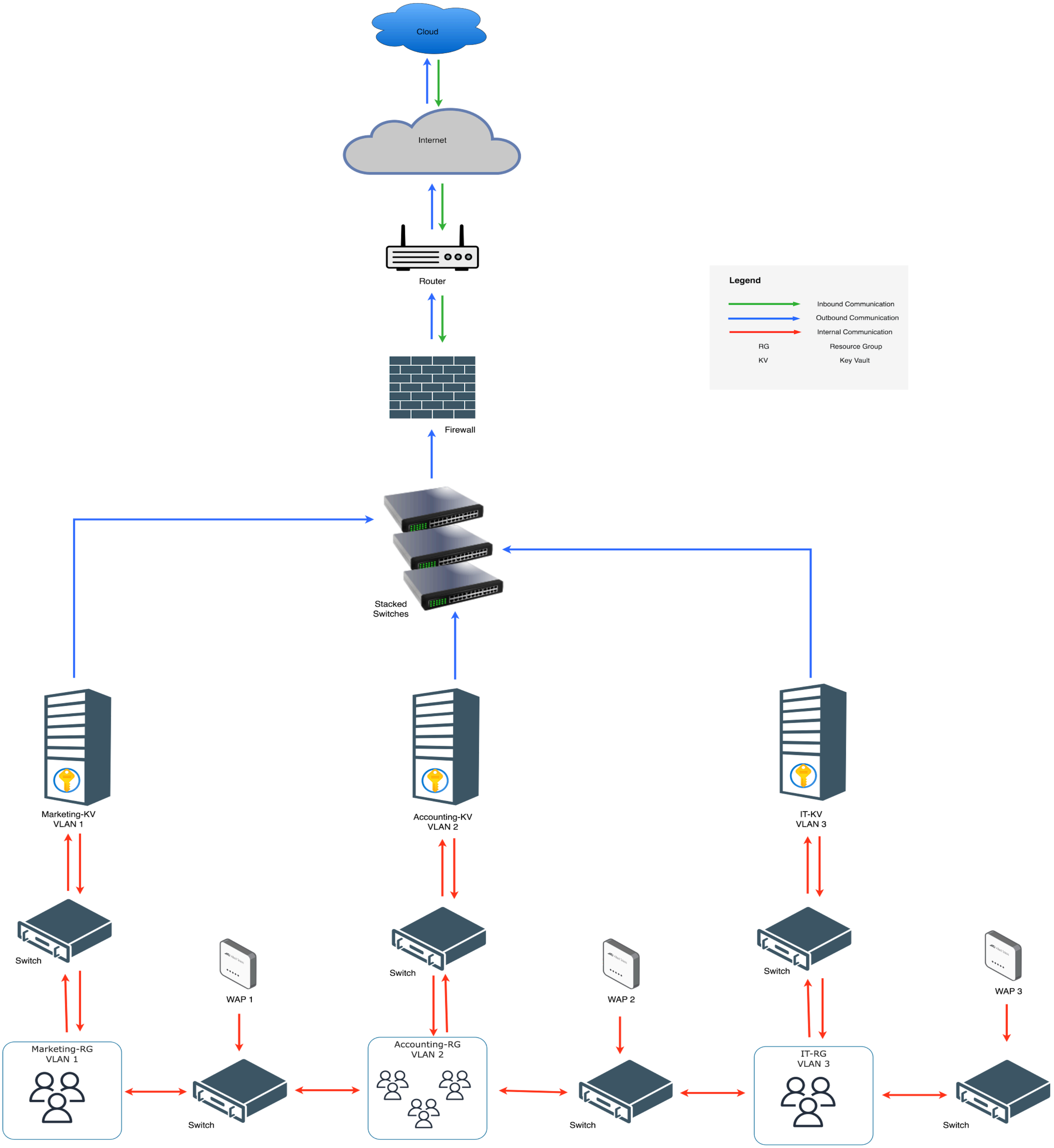
🟥	**Critical =**	High Impact + High Likelihood
🟧	**High =**	Medium Impact + High Likelihood or High Impact + Medium Likelihood
🟨	**Medium =**	Medium Impact + Low Likelihood or Low Impact + Medium Likelihood
🟩	**Low =**	Low Impact + Low Likelihood

Appendix B: Compliance Mapping Table:

Control	NIST Standard	PCI DSS Requirement	Gap	Risk Rating*	MITIGATION RECOMMENDATIONS
AC-6	Access Controls	PCI DSS Req. 7.1 - 7.2	No access control mechanisms are implemented	**High**	Configure Azure RBACs for department-specific resource groups (RGs); Assign key vault access policies per department; Implement network segmentation with VLANs for each RG to separate traffic
CP-9	Disaster Recovery	PCI DSS Req. 12.10.1 & 12.5.1	Data backups and recovery testing are not performed	**Critical**	Implement Azure daily backups for critical assets; configure a backup retention and recovery plan, per policy requirements; conduct quarterly restoration tests
RA-5	Vulnerability Scanning	PCI DSS Req. 11.2.x	No vulnerability management program is in place	**High**	Define vulnerability scanning scope for all internal/external IP ranges; Configure Azure Defender to run automated quarterly scans; Initiate scans upon major configurations and develop a plan to track and remediate any vulnerabilities

**The "Risk Rating" column retrieved ratings from Appendix A to highlight the urgency of implementing controls.*

Appendix C: Secure Network Topology Design


Cloud
Internet
Router
Firewall
Stacked Switches
Legend
Inbound Communication
Outbound Communication
Internal Communication
RG
Resource Group
KV
Key Vault
Marketing-KV
VLAN 1
Accounting-KV
VLAN 2
IT-KV
VLAN 3
Switch
Switch
Switch
WAP 1
WAP 2
WAP 3
Marketing-RG
VLAN 1
Switch
Accounting-RG
VLAN 2
Switch
IT-RG
VLAN 3
Switch