Azure Cloud Compliance Assessment - Simulated Project

This project was completed as part of a graduate-level Cybersecurity course and is based on a fictional company scenario. All names and details are for educational purposes only.

Field	Details
Date	July 2025
Type	Graduate Coursework Simulation
Role	GRC Analyst
Duration	~4 weeks

Project Summary

In this simulation, I acted as a GRC analyst who was responsible for identifying and mitigating compliance risks for a fictional government-contracted logistics company migrating to Microsoft Azure. The project focused on strengthening cloud security posture by mapping identified risks to NIST SP 800-53 and PCI DSS controls and delivering a remediation strategy to ensure compliance with both frameworks.

Key Achievements

- Identified and prioritized three compliance gaps in Microsoft Azure IaaS environment.
- Created a risk summary table with ratings and mitigation strategies.
- Mapped risks to NIST SP 800-53 and PCI DSS for multi-framework compliance readiness.

Skills Demonstrated

- Risk assessment & prioritization
- Compliance mapping, gap analysis and secure network topology design
- Azure-specific security recommendations
- Framework knowledge: NIST SP 800-53, PCI DSS and FISMA

Figure 1: Risk Summary Table

			RISK ASSESSMENT				
RISK ID	**TOPIC**	**RISK DESCRIPTION**	**IMPACT**	**LIKELI-HOOD**	**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

Figure 2: 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 backup or 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 adds ratings from Appendix A to highlight the urgency of implementing controls.*

Figure 3: Risk Rating Legend

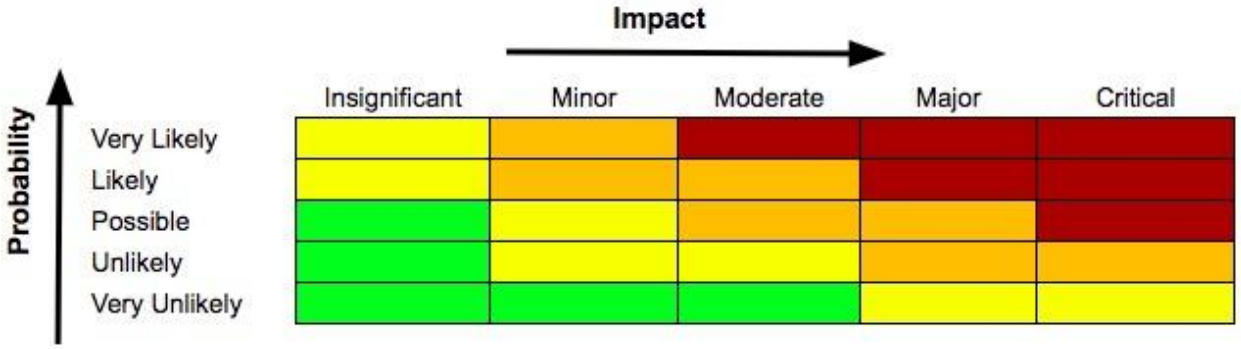
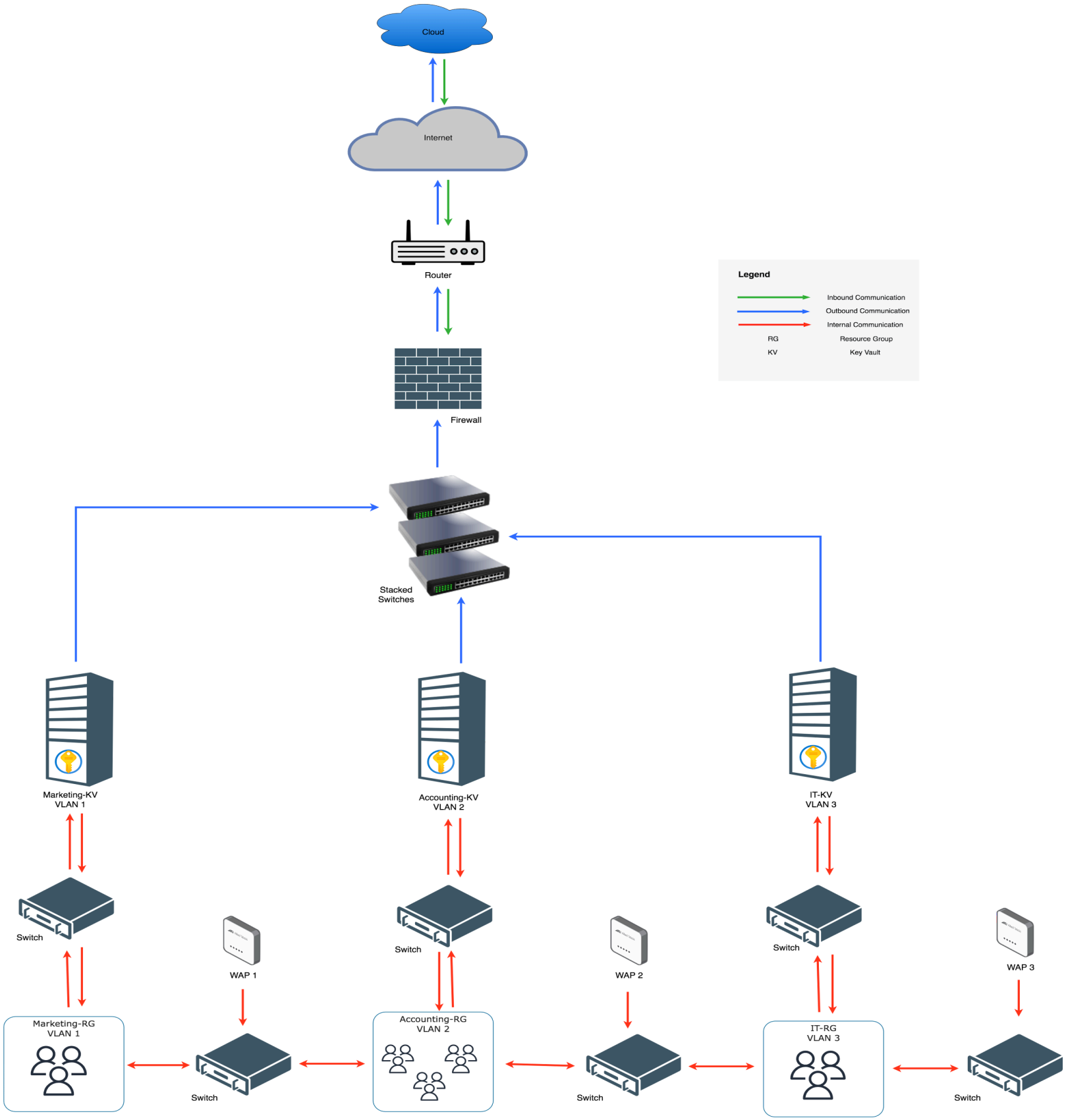


Figure 4: Secure Network Topology Design:



Learning Outcomes

This project strengthened my ability to assess cloud compliance risks, map controls across frameworks and recommend Azure-specific security measures. While fictional, it reflects the same methodologies used in real-world compliance assessments, enhancing my readiness for GRC and cloud security roles.

Full Report

Access the full report by visiting:
https://github.com/tnwoodard/azure-grc-simulation-project