PCI-DSS Compliance

GRC Case Study

Joshua T. Neuman

Table of Contents

I. Introduction/Executive Summary:

Timbuktu e-Group (TeG), a small e-Commerce company with an existing traditional network architecture is looking to gain Payment Card Industry-Data Security Standard (PCI-DSS) compliance for a pilot Microsoft Azure based cloud implementation project as a proof of concept. They would like to implement an internal Card Holder Data Environment instead of relying on third-party payment processors. They currently process payments through their web-app, which is handled by a 3rd party processor.

TeG has engaged Aegis Solutions to conduct a limited-scope assessment on their pilot Azure cloud infrastructure and has requested compliance against PCI-DSS v3.21, with recommendations where feasible for v4.0 compliance (required in 2024).

This case study will provide a snapshot across the 12 PCI requirements, with a particular focus on the IT infrastructure. In a real-world business environment, the IT infrastructure represents a fraction of the business' necessary considerations, which also include the people and processes involved in the handling and storage of Cardholder Data.

II. PCI-DSS Background:

The PCI-DSS security standards were initially created in 2004 by Visa, Mastercard, Discover Financial Services, JCB International and American Express. These standards are governed by the Payment Card Industry Security Standards Council (PCI-SSC). The goal of these standards is to protect against theft and fraud.

Though this body does not have the legal authority to compel compliance, all businesses which handle credit and debit card transactions must maintain compliance or face severe fines while non-compliant. Non-compliance also presents the risk of data breaches due to either non-existent or poorly implemented security practices across various areas of the business as described in the requirements below.

The PCI-DSS framework is composed of 12 requirements:

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data

2. Do not use vendor-supplied parameters for security defaults.

Protect Cardholder Data

3. Protect stored Cardholder data.

4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know.

8. Identify and authenticate access to system components.

9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

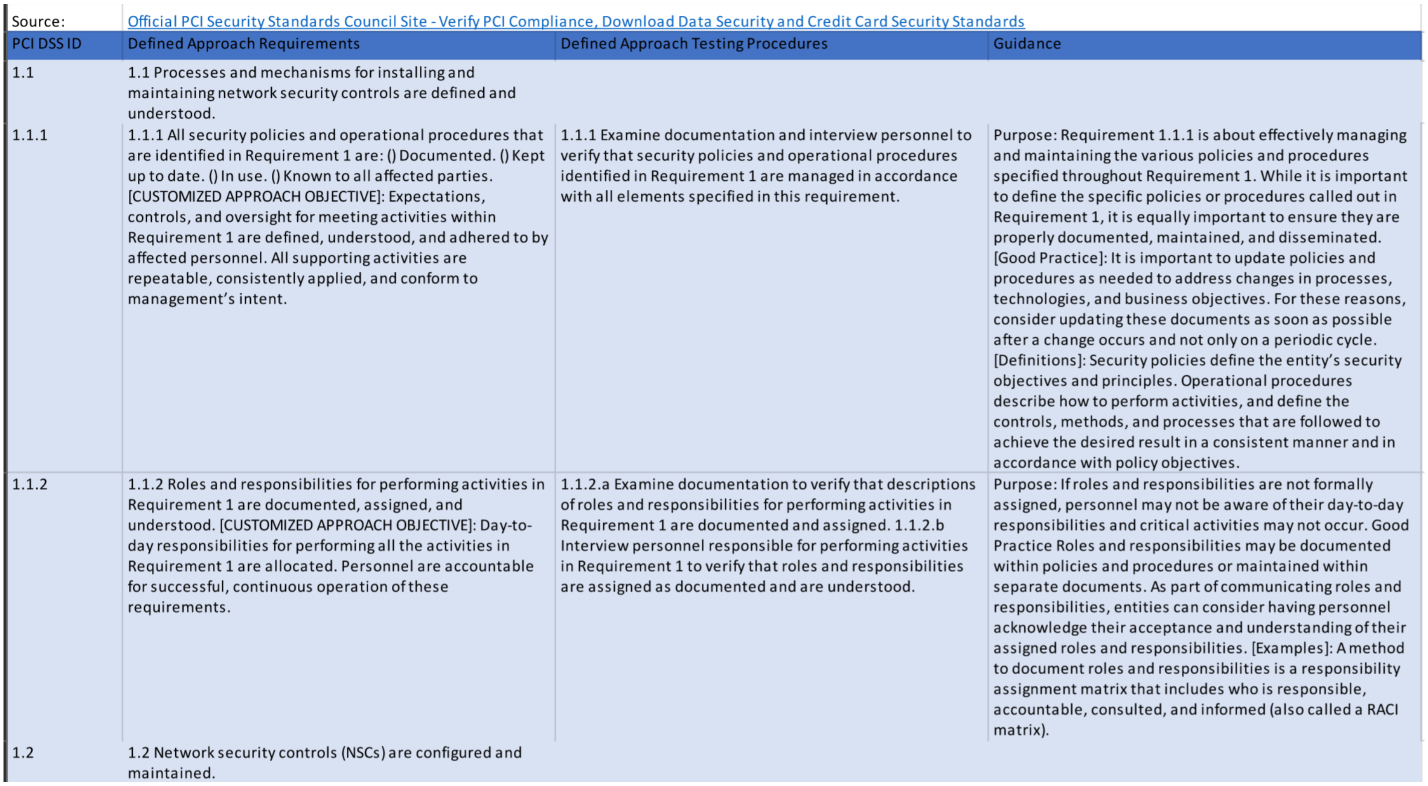
10. Track and monitor all access to network resources and cardholder data.

11. Regularly monitor and test networks

Maintain an Information Security Policy

12. Maintain an Information Security Policy for All Personnel.

These 12 requirements are divided into sub-requirements with a Descriptor, Control Description, Test Methodology, and Guidance:



Source: Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

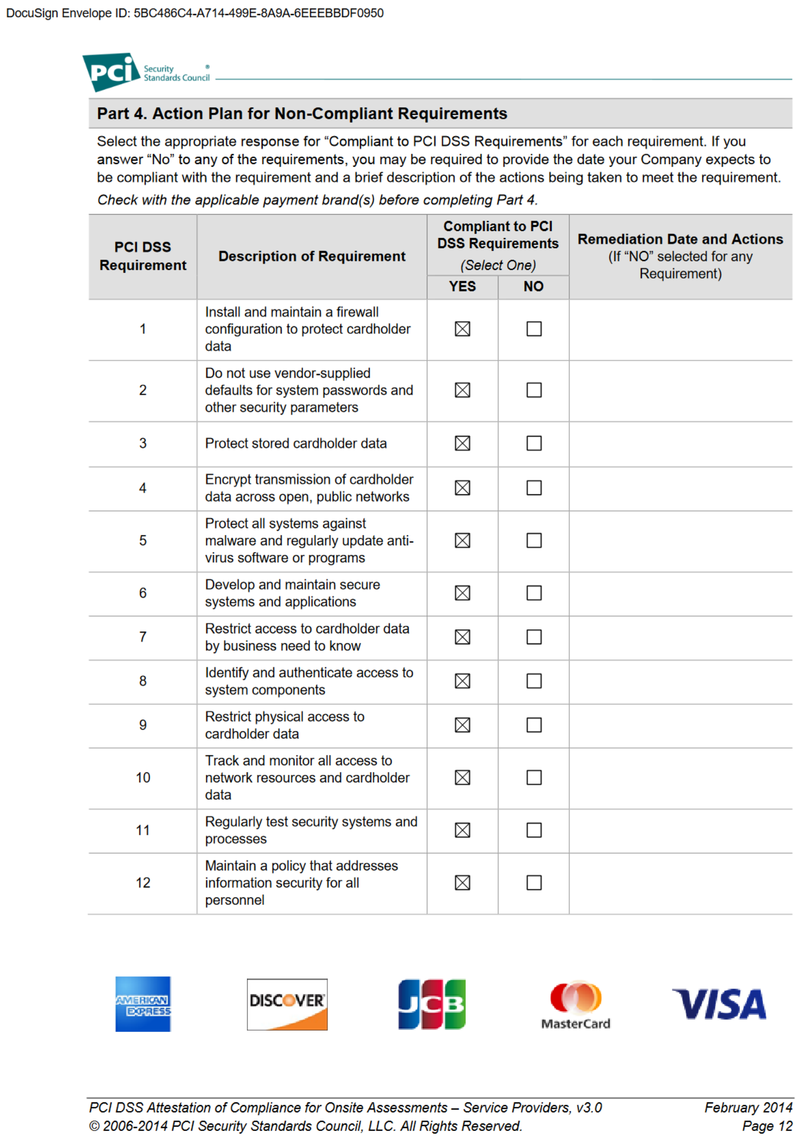
PCI DSS ID	Defined Approach Requirements	Defined Approach Testing Procedures	Guidance
1.1	1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.		
1.1.1	1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: () Documented. () Kept up to date. () In use. () Known to all affected parties. [CUSTOMIZED APPROACH OBJECTIVE]: Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	1.1.1 Examine documentation and interview personnel to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.	Purpose: Requirement 1.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 1. While it is important to define the specific policies or procedures called out in Requirement 1, it is equally important to ensure they are properly documented, maintained, and disseminated. [Good Practice]: It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. For these reasons, consider updating these documents as soon as possible after a change occurs and not only on a periodic cycle. [Definitions]: Security policies define the entity's security objectives and principles. Operational procedures describe how to perform activities, and define the controls, methods, and processes that are followed to achieve the desired result in a consistent manner and in accordance with policy objectives.
1.1.2	1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. [CUSTOMIZED APPROACH OBJECTIVE]: Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	1.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned. 1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.	Purpose: If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. Good Practice Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. [Examples]: A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).
1.2	1.2 Network security controls (NSCs) are configured and maintained.		

Figure 2-1: PCI-DSS Requirements Matrix Example.

Spreadsheets such as this are used both by the Enterprise administrators and responsible GRC personnel to track PCI-DSS compliance.   Ideally, Enterprise-wide GRC software solutions would be implemented to ease in tracking these artifacts. Solutions such as Qualys can also provide inventory control, vulnerability management automation, and Compliance validation (examples are provided in section V.)

III. Attestation of PCI-DSS Compliance from Cloud Provider (Microsoft Azure):

Providers of Cloud Infrastructure such as Microsoft Azure and Amazon Web Services are required to provide documentation that proves PCI-DSS certification. This certification shows the compliance of Microsoft's environment in general with PCI-DSS, and does not necessarily mean the business entity is compliant (as will be demonstrated in later sections).



DocuSign Envelope ID: 5BC486C4-A714-499E-8A9A-6EEEBBDF0950

PCI Security Standards Council

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (*Select One*)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☒	□	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	□	
3	Protect stored cardholder data	☒	□	
4	Encrypt transmission of cardholder data across open, public networks	☒	□	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	□	
6	Develop and maintain secure systems and applications	☒	□	
7	Restrict access to cardholder data by business need to know	☒	□	
8	Identify and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Track and monitor all access to network resources and cardholder data	☒	□	
11	Regularly test security systems and processes	☒	□	
12	Maintain a policy that addresses information security for all personnel	☒	□	

PCI DSS Attestation of Compliance for Onsite Assessments – Service Providers, v3.0 *February 2014*
© 2006-2014 PCI Security Standards Council, LLC. All Rights Reserved. *Page 12*

Figure 3-1: Snapshot of Microsoft's 2014 Azure AOC documentation.

*Note: 2014 Documentation URL: https://download.microsoft.com/download/7/1/E/71E02A19-D1A4-448F-8CEA-D6A19398ABDA/Azure%20PCI%20AOC%20Feb%202015.pdf

Current documentation resides behind a secured site requiring subscription: https://servicetrust.microsoft.com/DocumentPage/b9cc20e0-38db-4953-aa58-9fb5cce26cc2

IV. Defining the Cardholder Data Environment (CDE) Scope:

According to the PCI-DSS framework, the first step in the assessment process is to definite the scope of the CDE. TeG's initial cloud network diagrams are shown in Diagrams 1A: Initial Network Diagram 1B: CDE Data Flow.

TeG Network Diagrams:

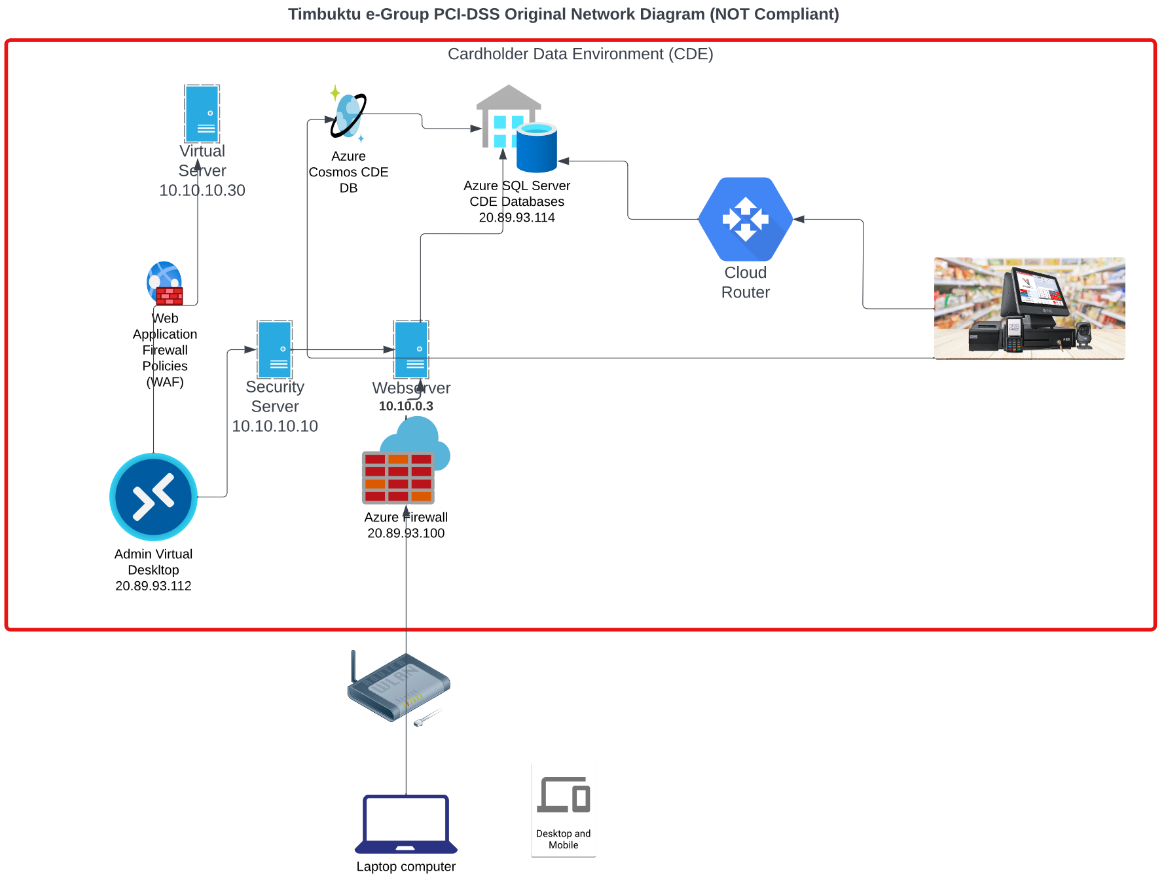

Timbuktu e-Group PCI-DSS Original Network Diagram (NOT Compliant)
Cardholder Data Environment (CDE)
Virtual Server 10.10.10.30
Azure Cosmos CDE DB
Azure SQL Server CDE Databases 20.89.93.114
Cloud Router
Web Application Firewall Policies (WAF)
Security Server 10.10.10.10
Webserver 10.10.0.3
Azure Firewall 20.89.93.100
Admin Virtual Desktop 20.89.93.112
Desktop and Mobile
Laptop computer

Figure 4-1: TeG Original Infrastructure Network Diagram (Not Compliant)

Recommended Revised Topology:

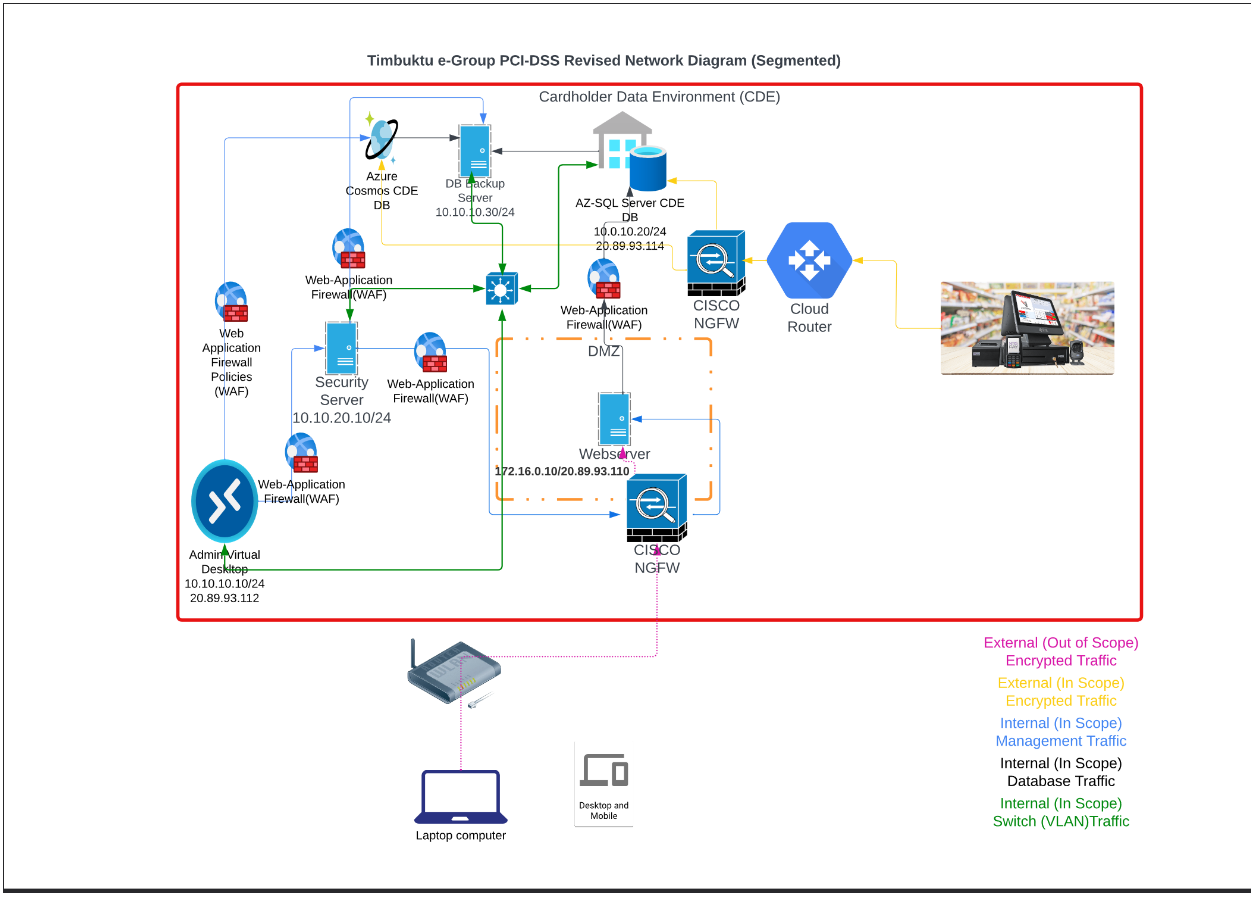

Timbuktu e-Group PCI-DSS Revised Network Diagram (Segmented)
Cardholder Data Environment (CDE)
Azure Cosmos CDE DB
DB Backup Server 10.10.10.30/24
AZ-SQL Server CDE DB 10.0.10.20/24 20.89.93.114
Web-Application Firewall(WAF)
Web Application Firewall Policies (WAF)
Web-Application Firewall(WAF)
CISCO NGFW
Cloud Router
Security Server 10.10.20.10/24
Web-Application Firewall(WAF)
DMZ
Webserver
172.16.0.10/20.89.93.110
Web-Application Firewall(WAF)
Admin Virtual Desktop 10.10.10.10/24 20.89.93.112
CISCO NGFW
Laptop computer
Desktop and Mobile
External (Out of Scope) Encrypted Traffic
External (In Scope) Encrypted Traffic
Internal (In Scope) Management Traffic
Internal (In Scope) Database Traffic
Internal (In Scope) Switch (VLAN)Traffic

Figure 4-2 In-Scope CDE Proposed Network Diagram (Segmented)

The existing infrastructure was built as a flat network, with zero network segmentation. While not explicitly listed as one of the 12 PCI-DSS requirements, network segmentation is a best security practice to isolate sensitive areas of the network (such as the Cardholder Data Environment – CDE).

The new topology is explicitly segmented into appropriate Virtual Local Area Networks (vlans) and Sub networks (subnets), while containing Firewalls (FW) to comply with Requirement #1: Install and maintain a firewall configuration to protect cardholder data.

Further, the CDE should only consist of the systems, people, and processes that directly involve the processing of cardholder data. Extraneous servers have been moved to a separate vlan and subnet.

V. Compliance Scan

A sample from the compliance scan run against the Windows Virtual Machine (Windows 10 Operating System) within the CDE using Qualys PCI scanner is included below:

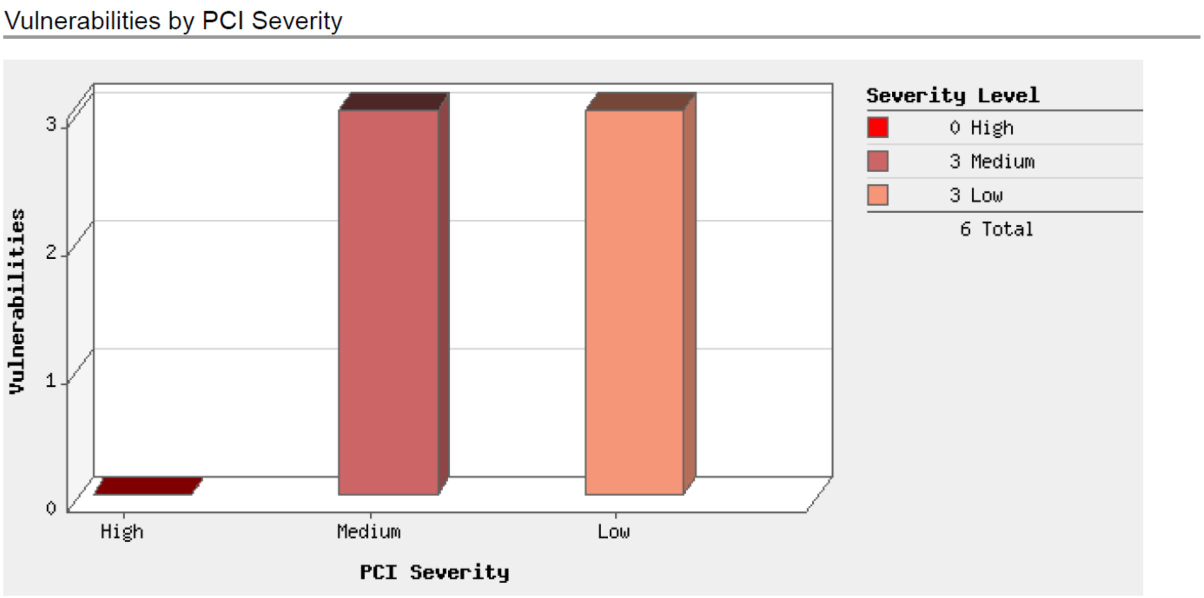
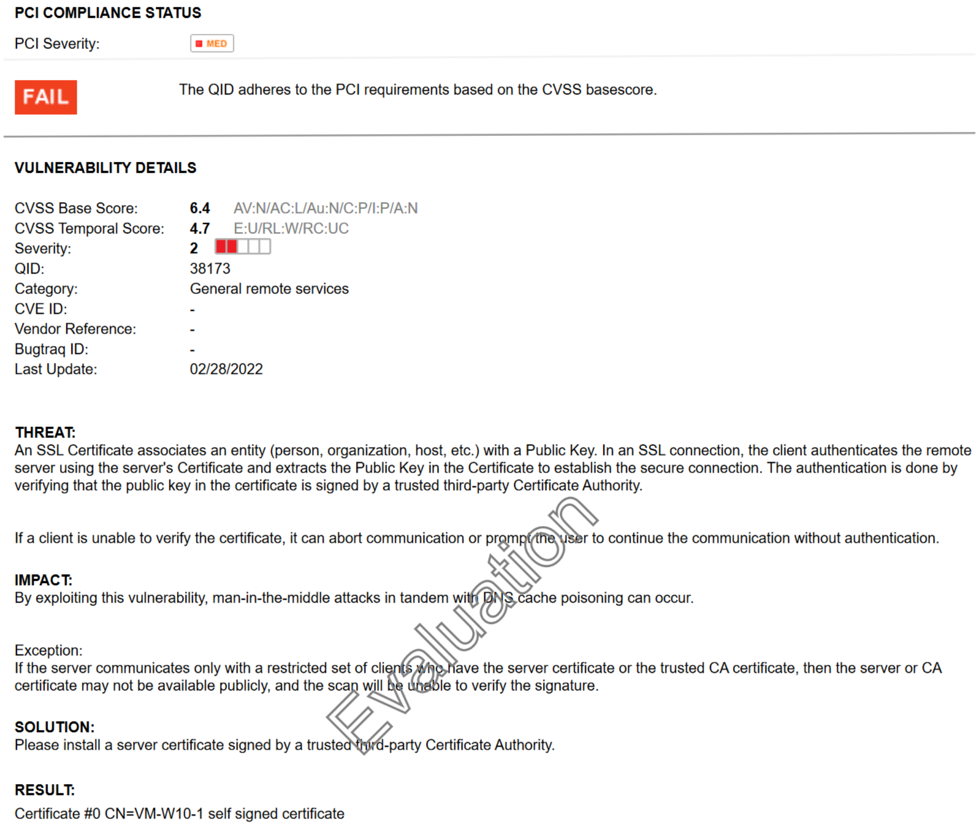


Figure 5-1: Qualys PCI Compliance Scan Vulnerability Severity Levels



PCI COMPLIANCE STATUS

PCI Severity: ■ MED

FAIL The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score:	**6.4** AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	**4.7** E:U/RL:W/RC:UC
Severity:	**2** ■■□□□
QID:	38173
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	02/28/2022

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

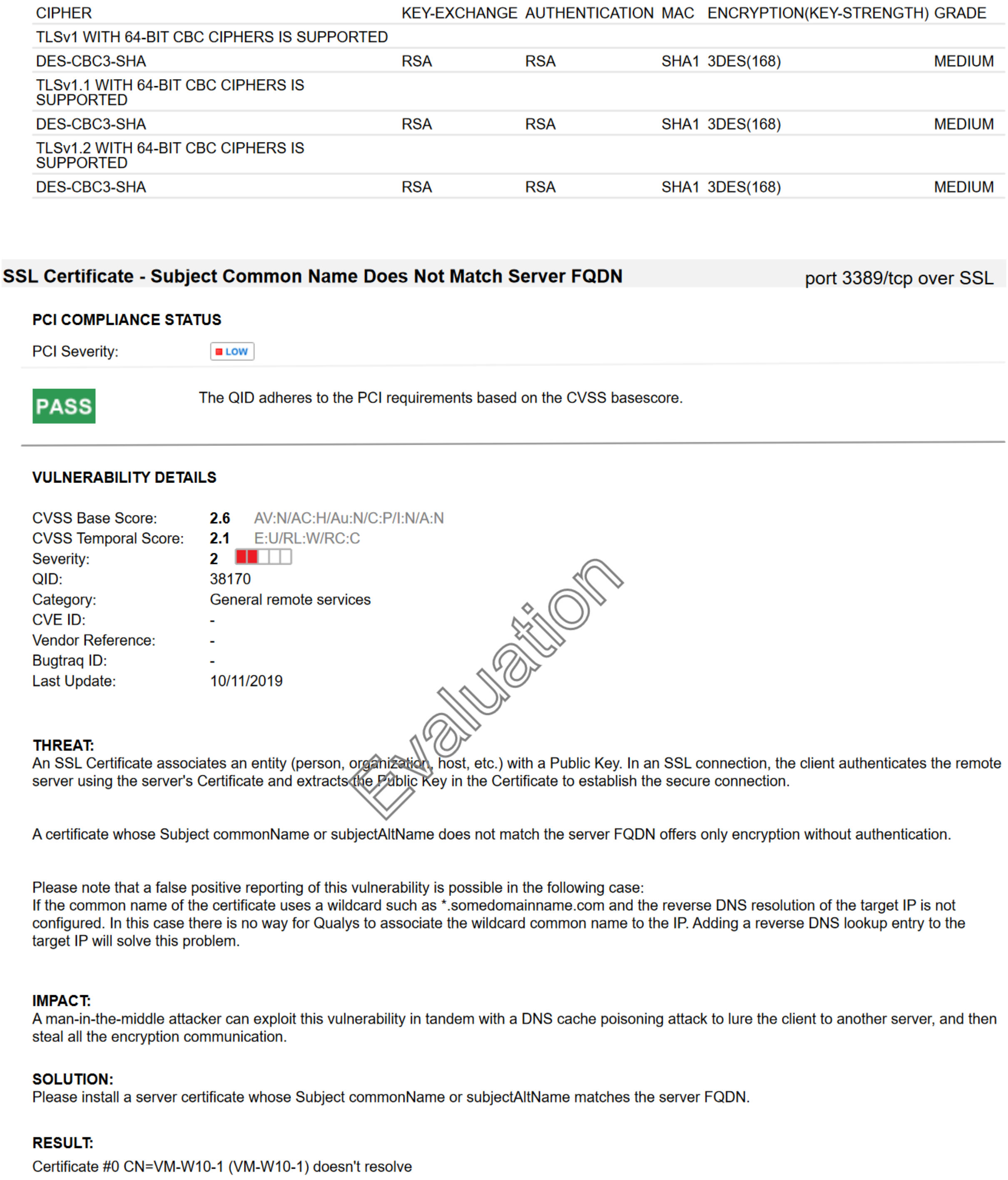
IMPACT:
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:
Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:
Certificate #0 CN=VM-W10-1 self signed certificate

Figure 5-2: Self-Signed Certificate in use resulting in Compliance Failure.



CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM

SSL Certificate - Subject Common Name Does Not Match Server FQDN port 3389/tcp over SSL

PCI COMPLIANCE STATUS

PCI Severity: LOW

PASS The QID adheres to the PCI requirements based on the CVSS basescore.

VULNERABILITY DETAILS

CVSS Base Score:	**2.6**	AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1**	E:U/RL:W/RC:C
Severity:	**2**	
QID:	38170	
Category:	General remote services	
CVE ID:	-	
Vendor Reference:	-	
Bugtraq ID:	-	
Last Update:	10/11/2019	

THREAT:
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

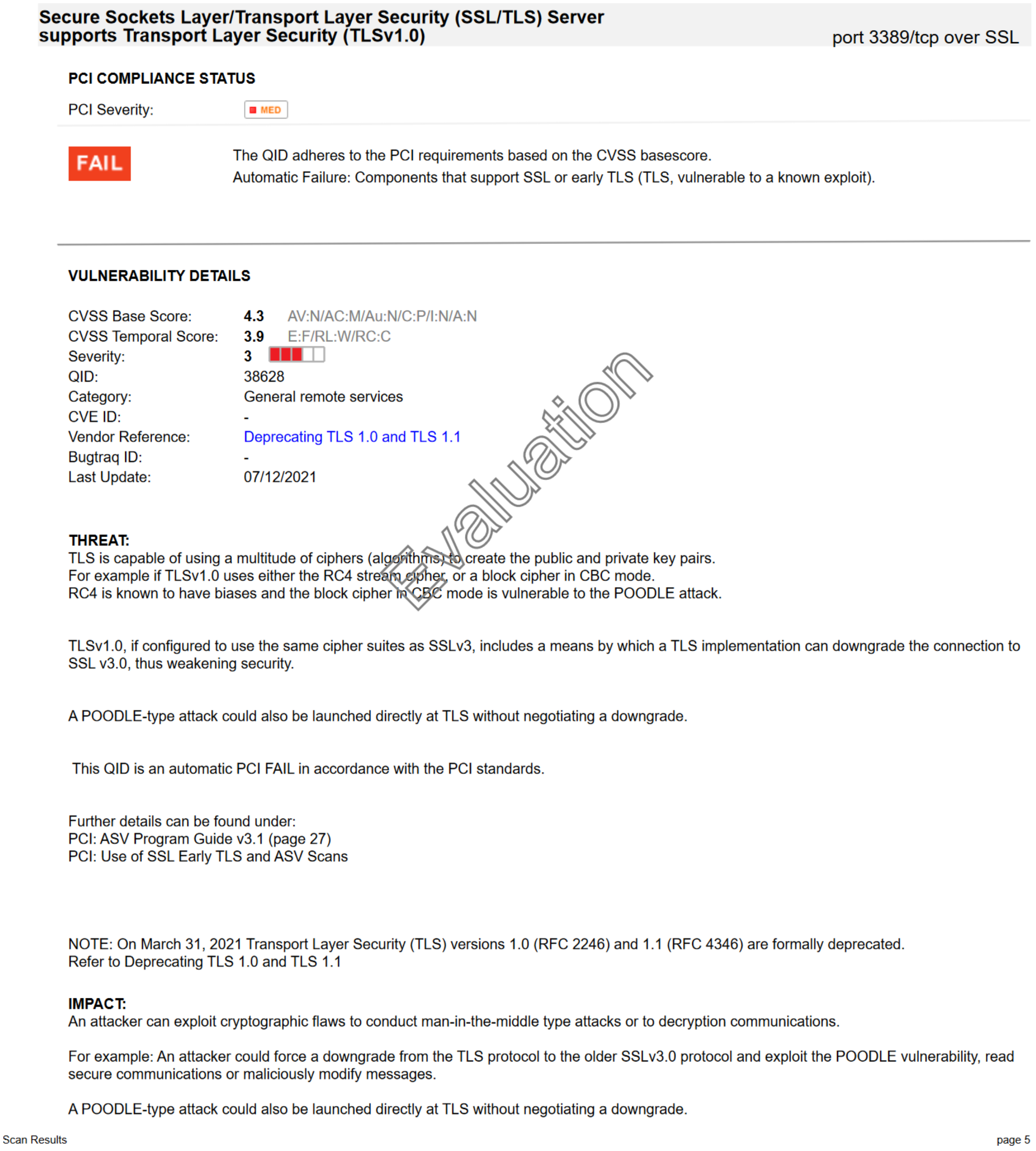
IMPACT:
A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:
Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:
Certificate #0 CN=VM-W10-1 (VM-W10-1) doesn't resolve

Figure 5-3:SSL Certificate Common Name does not match Server Fully Qualified Domain Name

This vulnerability is due to a mismatch between the server's SSL certificate and the server's FQDN. Though it is still PCI Compliant.



Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) port 3389/tcp over SSL

PCI COMPLIANCE STATUS

PCI Severity: ■ MED

FAIL

The QID adheres to the PCI requirements based on the CVSS basescore.
Automatic Failure: Components that support SSL or early TLS (TLS, vulnerable to a known exploit).

VULNERABILITY DETAILS

CVSS Base Score:	**4.3**	AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9**	E:F/RL:W/RC:C
Severity:	**3**	■■■□□
QID:	38628	
Category:	General remote services	
CVE ID:	-	
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1	
Bugtraq ID:	-	
Last Update:	07/12/2021	

THREAT:
TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27)
PCI: Use of SSL Early TLS and ASV Scans

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated.
Refer to Deprecating TLS 1.0 and TLS 1.1

IMPACT:
An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

Scan Results page 5

Figure 5-4: Non-Compliance due to SSL/TLS v1.0 use.

SSL/TLS versions below 1.3 are considered insecure for the purposes of PCI data transmission.

This scan shows baseline PCI-DSS compliance has been achieved on some aspects of this virtual machine. However, it also shows several vulnerabilities related to PCI-DSS Requirement #3: Protect Cardholder Data.

Vulnerabilities:

A self-signed certificate and a deprecated SSL/TLS version is in use. These vulnerabilities potentially expose Cardholder Data to compromise, as TLS versions lower than 1.3 are no longer considered secure, and Certificates should be issued and signed by a Trusted Certificate Authority.

The VM is vulnerable to both Man in the Middle (MiTM) and POODLE attacks.

Recommended Remediations:

Requirement 2.23 (also Appendix A.2.1) - Enable TLS v1.3 on the Virtual Machine

Requirement 4.1.1 – Provision a Certificate for web browser traffic from a Trusted Certificate Authority.

VI. Requirement Snapshots – Vulnerabilities & Suggested Remediations

Requirement 1: Install and maintain a firewall configuration to protect cardholder data – Not fully cmpliant in the original cloud infrastructure. Recommend installing both Hardware (cloud-based) Cisco Next Generation Firewall (or comparable vendor such as Palo Alto, Fortigate etc.), in addition to Web Application/Host-based firewalls.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters – Compliant. Default passwords are not allowed by policy, when a new user (admin and non-admin) logs in for the first time, they must set a new strong password in order to gain access to TeG systems.

Requirement 3: Protect stored Cardholder Data - Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. Recommendation – Ensure data other than PAN, Expiry date, and Service code are not stored. To minimize risk, store only these data elements as needed for business.

Requirement 4: Encrypt transmission of Cardholder Data across open, public networks – Recommend implementation of TLS v1.3 on all web capable systems, in addition to Virtual Private Networks (VPNs) on systems connecting to the CDE.

Requirement 5: Protect all systems against malware and regularly update antivirus software – Recommend implementation of Cisco Next Generation Firewall (IPS/Adaptive functionality capable including Antivirus/malware), in addition to implementing Host Based Antivirus solution through Azure, or appropriate third-party vendor.

Requirement 6: Develop and maintain secure systems and applications – Vulnerability potentially Non-compliant. Software Development and Security Teams need to conduct a code review on the organization's Webapp.

Remediation – Implement PCI/DSS and Software Development Lifecycle/Security Best Practices.

Requirement 7: Restrict access to cardholder data by businesses need to know – Vulnerability Non-compliant, some employees who do not have payment responsibilities have had access to CDE on the legacy infrastructure.

Remediation – Implement Role Based Access Control (RBAC)on all CDE connected assets.

Requirement 8: Identify and Authenticate Access to User Components – Vulnerability Non-compliant due to lack of Multifactor Authentication (MFA). (This is required in PCI-DSS v4)

Remediation - Enable MFA on All Non-Console access for Administrators of CDE devices.

Requirement 9: Restrict Access to Cardholder Data – Physical Media related to cardholder data currently stored in a secured area on premises. Recommend migrating/backing up this data for redundancy and retention purposes via Azure Database solutions, or possibly a second provider such as AWS for high availability.

Requirement 10: Track and Monitor All Access to Cardholder Data – Recommend implementation of Azure Logging services such as Sentinel. Other Security Event Managers should be evaluated such as VMWare Carbon Black, and Splunk Enterprise. Specific PCI-DSS software should be evaluated as well.

Requirement 11A: Vulnerability Scans – Informed that scans run on legacy infrastructure monthly. Recommend increasing frequency to weekly, if possible, to mitigate the risk of extended zero-day vulnerability exposure. Recommend looking at Azure solutions

Requirement 11B: Penetration Test – Informed that Penetration testing was not conducted on legacy infrastructure by an external party. Penetration testing was conducted by the internal security team on an annual basis due to the size of the organization and associated costs. Pen-test has not been conducted on this pilot cloud infrastructure, due to the proof-of-concept nature of the project. Recommend partnering with an external Penetration Testing Consultancy once the full implementation phase is reached.

Requirement 12: Update Documentation and Conduct Risk Assessments – TeG's Security Policy should be updated with the following documents in mind: Employee Manuals, Policies and Procedures, Technology Usage Policies, Third-Party Vendor Agreements, Business Continuity, and Incident Response Plans. A robust security policy, which is regularly tested and updated is recommended, in addition to a strong cybersecurity training program for both employees and customers where appropriate.

Data Breach Fines	
Merchant processor compromise fine	$5,000-$50,000
Card brand compromise fees	$5,000-$500,000
Forensic investigation	$12,000-$100,000
Onsite QSA assessments following the breach	$20,000-$100,000
Free credit monitoring for affected individuals	$10-$30 per card
Card re-issuance penalties	$3-$10 per card
Security updates	$15,000+
Lawyer fees	$5,000+
Breach notification costs	$1,000+
Technology repairs	$2,000+
TOTAL Possible Cost	$50,000-$773,000

Table 6-1: Data Breach Fine Example (Categories and cost figures courtesy of Security Metrics)

VII. Tentative Roadmap:

Week 1– Remediate TLS and Certificate vulnerabilities across enterprise assets.

Update appropriate security policies and procedures while implementing vulnerability scans across enterprise assets. (Internal IT Administrators/Security team)

30 Days – Test and Network Implement architecture revisions, consulting with Microsoft and other third party vendors as needed for customized/cost-effective solutions.

Test and Implement Logging solution

60 Days – Test and Implement Multi-cloud solution for Cardholder Data backup/redundancy.

Implement Quarterly vulnerability scans from an external provider.

90 Days – Schedule Penetration Test with a third-party agency.

6 Month – Migrate from legacy architecture to cloud environment.

7 Months - Conduct an internal audit of Enterprise systems and processes.

6-9 Months – Re-engage QSA for official PCI-DSS audit preparation/engagement.

12 Months – Compliance

*** On-going** Cybersecurity Program Development (Employee training), Policy updates, Threat Intelligence, etc.

******Schedule subject to change based on testing and implementation results, meetings, and buy-in from the relevant Sr. Management/C-Suite stakeholders.

VIII. Self-Assessment Questionnaire (SAQ D) Snapshot:

The SAQ (probably type D in the case of TeG) SAQ D applies to merchants who don't meet the criteria for any other SAQ type. This SAQ type handles merchants who store card information.

Examples of SAQ D merchant types include:

- E-commerce merchants who accept cardholder data on their websites.

- Merchants with electronic storage of cardholder data.

- Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type.

- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

Examples of Questions include:

Is there a formal process to validate and test changes to all network connections, firewall, and router configurations? Yes

Are default passwords changed during setup? Yes

Does all cardholder data stored meet the requirements defined in the data retention policy? Yes

Can only personnel with a valid business need to see the PAN? No (Remediating)

Is PAN data masked when shown? Yes

Is all the information on the magnetic stripe on the back of a card stored on a disk or elsewhere after authorization? (Investigating)

Is information security included in the software development lifecycle? Yes (Validating)

Are access control systems in place in all system components? No (Remediating)

Is there a mechanism to find vulnerabilities? Yes

Are there quarterly external network vulnerability scans? No (Scheduling IAW Roadmap)

Is information from reliable outside sources used for vulnerabilities? Yes

Do authorized parties approve the required privileges? Yes

Is multi-factor authentication used for remote network access? Yes

IX. Conclusion:

This case study illustrated an initial assessment of a pilot cloud PCI-DSS implementation, from CDE scoping to snapshot compliance scan, vulnerability assessment, and recommended remediations, along with a roadmap of milestones. Assessments of the 12 PCI Requirements were conducted, though one specific aspect was chosen for each requirement. A snapshot of the SAQ was also provided with answers mirroring the scenario.

The scenario described in this case study represents a limited scope/snapshot Governance, Risk Management, and Compliance (GRC) engagement based on PCI-DSS compliance. Qualys PCI and Microsoft Azure Cloud services were used as much as practical in the creation of this study to provide a flavor for a real-world engagement. While realistic, the scope is limited due to the time and cost constraints of conducting a comprehensive assessment against a fully realized enterprise architecture.

X. References:

1. PCI-DSS Official Site:

https://www.pcisecuritystandards.org/

2. PCI-DSS Information Repository:

https://pcidss.com/

3. Qualys (PCI Compliance Scanner):

https://www.qualys.com/solutions/pci-compliance/

3. Microsoft Azure PCI-DSS Regulatory Compliance Built-In Initiative:

https://learn.microsoft.com/en-us/azure/governance/policy/samples/pci-dss-3-2-1

4. Security Metrics:

https://www.securitymetrics.com/

5. Cisco Systems:

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

6. Compliance Quickstart (PCIDSS Spreadsheet):

https://www.compliancequickstart.com/