BDO KNOWS:

CYBERSECURITY

CYBERSECURITY FOR THE PAYMENT CARD INDUSTRY

INTRODUCTION: THE COUNCIL

The Payment Card Industry Security Standards Council (PCI SSC) is a governing organization that develops and maintains security standards for the protection of cardholder data. The standards are a global framework that were introduced in 2006 and was derived from the individual data security compliance programs of five major payment brands: American Express, Discover Financial Services, JCB International, MasterCard, and Visa.

This is an excerpt from *Cybersecurity in the Digital Age*. To learn more about PCI please contact:

FRED BRANTNER
Director, Cybersecurity Advisory Services
fbrantner@bdo.com

GREGG GARRETT
Head of U.S. and International Cybersecurity Advisory Services
ggarrett@bdo.com

GREG SCHU
Partner, Cybersecurity Advisory Services
gschu@bdo.com

The PCI SSC is independent of the payment brands and is responsible for the development, management, education, and awareness of the PCI Security Standards.
In addition to the security standards, the Council maintains a list of frequently asked questions, new material pertaining to the security standards, and rosters of Internal Security Assessors (ISAs), Qualified Security Assessors (QSAs), Payment Application Qualified Security Assessors (PA-QSA), Point-to-point QSAs, PCI Professionals (PCIPs) and Qualified Integrators & Resellers (QIRs). For additional information regarding the Council and the supported resources of the Council, visit their website **here**.

PCI DATA SECURITY STANDARDS (DSS)

PCI Data Security Standards (PCI DSS) is a set of standards developed and maintained by the PCI SSC and were designed for the security of the cardholder data environments that process, store, or transmit account data. This also includes systems that could affect the security of the cardholder data environment. These standards are referred to as requirements and apply to all entities involved in payment card processing including merchants, processors, acquirers, issuers, and service providers as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. PCI DSS compliance validation is required every 12 months.

Cardholder data and sensitive authentication data are defined as follows:

Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
▶ Primary Account Number (PAN) ▶ Cardholder Name ▶ Expiration Date ▶ Service Code	▶ Full track data (magnetic-stripe data or its equivalent on a chip) ▶ CAV2/CVC2/CVV2/CID ▶ PINs/PIN blocks

There are six (6) primary domains and twelve (12) PCI DSS requirements. The primary domains and PCI DSS requirements are:

PCI Primary Domains	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	▶ Install and maintain a firewall configuration to protect data. ▶ Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	▶ Protect stored cardholder data. ▶ Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	▶ Protect all systems against malware and regularly update antivirus software or programs. ▶ Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	▶ Restrict access to cardholder data by business need-to-know. ▶ Identify and authenticate access to system components. ▶ Restrict physical access to cardholder data.
Regularly monitor and test networks	▶ Track and monitor all access to network resources and cardholder data. ▶ Regularly test security systems and processes.
Maintain an information security policy	▶ Maintain a policy that addresses information security for all personnel.

Each requirement has its own set of controls to be tested and the number of controls tested depends on the scope of the assessment. An example for this would be, if an organization does not perform system development and the QSA verified through interviews, observations and testing procedures that the organization does not develop software, then a majority of requirement six (6) would be not applicable.

The PCI DSS requirements are broken up into different sections: Testing Procedures, Reporting Instructions, Assessor's Responses, and Summary of Assessment Findings. Within each requirement, there are sub requirements. See below for an example of requirement 5.1.

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessments Findings (check one)				
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).			In Place ☐	In place w/CCW ☐	N/A ☐	Not Tested ☐	Not in Place ☐
5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	**Identify the sample** of system components (including all operating system types commonly affected by malicious software) selected for this testing procedure.						
	For each item in the sample, **describe how** anti-virus software was observed to be deployed.						

Think of the testing procedure as a control objective. The PCI DSS is validated against this control objective. The reporting instruction is to be viewed as the guidance to make sure the objective of the testing procedure is met. The reporting instructions could be a review of a policy or procedure, an interview with an applicable individual, or an observation of a process or procedure. In many cases, the reporting instructions will entail all these processes to meet the requirement of the testing procedure.

The reporting details are the assessor's (QSAs) response where the assessor will document who they interviewed, which policy and procedure they reviewed, the conclusions of their observations, and the result of their testing to satisfy the testing procedures.

The summary of the assessment findings is simply a check box where the assessor will note if the requirement is in place, in place with a compensating control, not applicable, not tested, or not in place. The assessor will mark one of these boxes and the mark must align with what the assessor wrote under the assessor's response section.

REPORT ON COMPLIANCE (ROC)

The Report on Compliance (ROC) is a completed PCI DSS assessment of an organization's cardholder environment and includes the executive summary, PCI DSS requirements and sub-requirements, and appendix. The executive summary section is a description of how the entity accepts payment cards for business transactions and includes how and why the organization stores, processes, and/or transmits cardholder data. The PCI DSS requirements/sub-requirements are the testing procedures of the organization's cardholder data environment. The appendix contains additional PCI DSS requirements for different types of entities.

A level 1 entity is a classifiaction for merchants that has over 6 million Visa or MasterCard transactions annually and for all service providers. Level 1 entities are required to complete a ROC that is accompanied by an Attestation of Compliance (AOC). The QSA company will assess the organization's PCI DSS requirements and issue the ROC and AOC to the organization if they are a merchant and will issue only the AOC to the acquirer or payment brand if the assessed entity is a service provider. The QSA will provide the ROC to the acquirer and payment brand when requested.

SELF ASSESSMENT QUESTIONNAIRE (SAQ)

The Self Assessment Questionnaire (SAQ) is like a ROC in that it has an executive summary, PCI DSS requirements and sub-requirements, and an appendix. The SAQ uses the same twelve (12) PCI DSS questions and testing procedures; however, the results of the testing procedures are not written out in detail. The results are recorded in a check box to indicate if the requirement is in place, in place with a compensating control, not in place, or not applicable.

A level 2, 3, or 4 entity is a classifiaction for merchants that have less than 6 million Visa or MasterCard transactions annually. Level 2, 3, or 4 entities may perform a self-assessment of their PCI environment as long as the SAQ and accompanying AOC are signed off by an authorized signing officer of the organization being assessed. The SAQ does not need to be completed by a QSA; however, a QSA can assist and sign off on an organization's SAQ.

For further detailed information on classification levels, please reference Visa, MasterCard, or the PCI Council's websites: www.visa.com; www.mastercard.com; www.pcisecuritystandards.org