RESEARCH ARTICLE OPEN ACCESS

Analysis of Payment Card Industry Data Security Standard [PCI DSS] Compliance by Confluence of COBIT 5 Framework

Ashish Ukidve[1], Ds S SMantha[2], Milind Tadvalkar[3]
[1]*Principal, Vidyalankar Polytechnic, Mumbai, India*
[2]*Ex-Chairman, AICTE, Professor, VJTI, Mumbai India*
[3]*Director, Vidyalankar Dnyanapeeth Trust, Mumbai, India*

ABSTRACT
The Payment Card Industry Data Security Standard (PCI DSS) aims to enhance the security of cardholder data and is required when cardholder data or authentication data are stored, processed or transmitted. The implementation of enabling processes from COBIT 5 can complement compliance to PCI DSS. COBIT 5 assists enterprises in governance and management of enterprise IT and, at the same time, supports the need to meet security requirements with supporting processes and management activities. This paper provides analysis of mapping of COBIT 5 supporting processes to PCI DSS 3.0 security requirements. It also presents domains which support the simultaneous application of COBIT 5 and PCI DSS 3.0 which would help create collaborations within the enterprise.

I. INTRODUCTION

PCI DSS

PCI DSS was released by the PCI Security Standards Council (PCI SSC), comprising of a panel of five global payment brands—Discover Financial Services, American Express, JCB International, Visa and MasterCard Worldwide Inc. PCI DSS also contains requirements for data security and related audit methods.

The goal of PCI DSS is primarily to protect the confidentiality of cardholder data. Confidentiality is the assurance that data cannot be viewed by or disclosed to unauthorized persons and, thus, be compromised. Confidentiality, as part of the information security triplet that includes availability and integrity, is one of the main goals of information security. Measures that are used to protect confidentiality frequently also protect integrity. For example, if data are compromised by an attacker, integrity will often be affected, too.

Integrity is the assertion that data remain accurateand complete and cannot be tampered with by unauthorized means. Availability means authorized systems or userscan access data at anyrequired time. The availability isassured by the systems andinfrastructure, which are ready for useand have adequate capacity to processall requests as quickly as necessary.

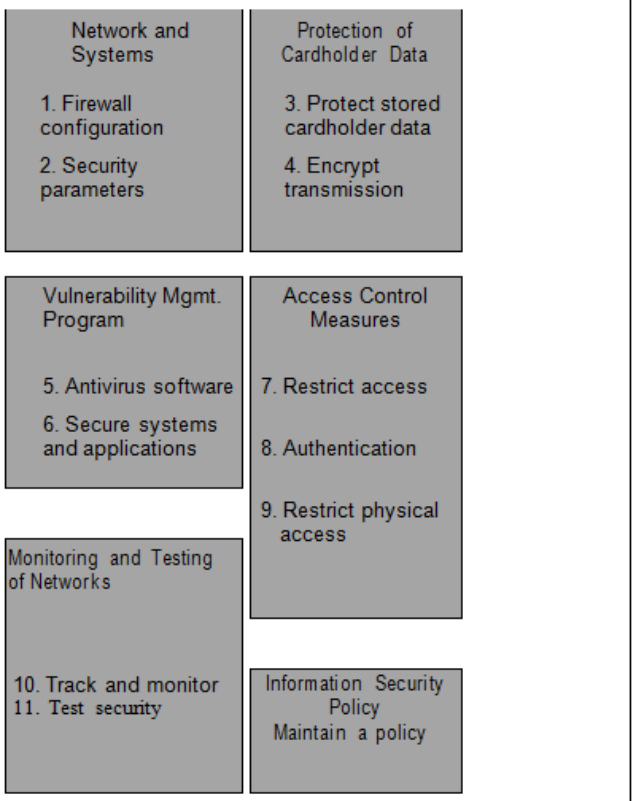
Attackers can compromise the information availability by overflowing asystem with service requests and, thus cause a denial-of-service attack, preventing access to information or data.

For card processing enterprises the setup of a PCI-DSS compliantenvironment is necessary becausewithout it a significant part of theirbusiness model would not be attainable and major losses would be incurred. In addition, loss of goodwill and possible fines by credit card companies can be expected. The credit card processing companies are classified into four compliance tiers (one to four) relating to the number of transactions affected over a 12-month period.Each tier has specific PCI DSS compliance requirements.

Organizations that are classified in tiers two to four must perform an annual self-assessment questionnaire (SAQ) and carry out a quarterly network scan by an approved scanning vendor .Enterprises with an annual number of transactions of six million or more are classified as tier one and must prepare an annual report on compliance (ROC) and be audited by a Qualified Security Assessor (QSA). The report of the audit is documented with an attestation of compliance (AOC).

The PCI DSS addresses 12 main requirements (fig 1) for control measures that are divided into topics which include network, protection of cardholder data, vulnerability management program, access control measures, monitoring and testing of networks and information security policy. Each requirement is further divided into sub-requirements and testing procedures.

Fig 1—PCI DSS 3.0 Topics and Requirements



In November 2013, version 3.0 of PCI DSS was published. By 2015, compliance to this new version will be obligatory for all card-processing companies. In comparison to version 2.0, version 3.0 contains additional clarifications, guidance and advanced requirements.The 20 advanced requirements are aimed at attaining improvements in the areas of awareness, security responsibility and flexibility.

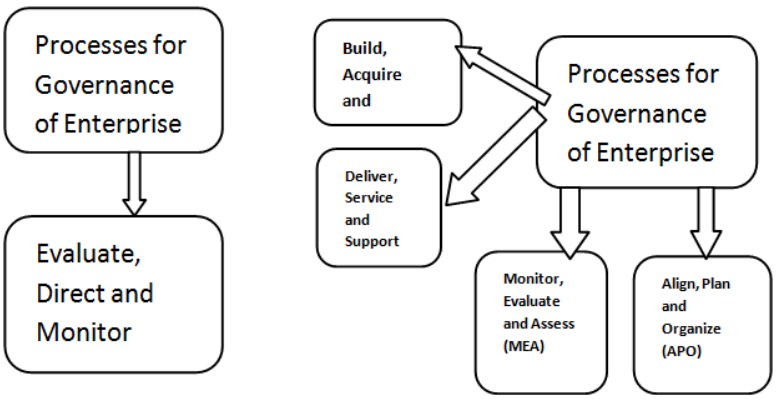
COBIT 5

COBIT 5 provides a comprehensive framework that assists enterprises in attaining their objectives for GEIT. It helps enterprises strike a balance between realizing benefits and optimizing risk levels and resource use.

The COBIT 5 product family includes enabler guides,professional guides and a collaborative online environment and provides a comprehensive IT governance framework.

In this paper we have mapped the PCI DSS 3.0 security requirements to the associated COBIT 5 supporting processes. The COBIT 5 process reference model includes processes for GEIT (fig 2)

Fig 2—COBIT 5 Process Reference



COBIT Enabling Processes by PCI DSS Topics
Network processes

All sensitive systems must be secured against unauthorized access fromuntrusted networks. Firewalls are used for securely isolating networks. Theycontrol and monitor the network traffic and block unwanted access between networks. They can be dedicated systems within the network infrastructure used or can be implemented locally on workstations.

Use of proper configurations can reduce the risk of unauthorized access from outside of the perimeter of company network.

System defaults that are present upon delivery of systems and components pose a security risk. A variety of unwanted services are usually activated after the initial installation of operating systems.These services can also be exploited by unauthorized users.

Passwords and other settings that were specified by the manufacturer of the systems are widely available and can be exploited by unauthorized user. Key enabling processes in COBIT 5 that can help mitigate risk are listed in fig 3.

Fig 3— Mapping of Network Processes
PCI DSS 3.0 Requirement *1. Install and maintain a firewall configuration to protect cardholder data*
COBIT 5 Process APO01.08 Maintain compliance with policies and procedures. APO03.02 Define reference architecture. APO12.01 Collect data. BAI03.03 Develop solution components. BAI03.05 Build solutions. BAI03.10 Maintain solutions. BAI06.01 Evaluate, prioritize and authorize change requests. BAI07.03 Plan acceptance tests. BAI07.05 Perform acceptance tests. BAI10.01 Establish and maintain a configuration model. BAI10.02 Establish and maintain a configuration repository and baseline. BAI10.03 Maintain and control configuration items. DSS01.03 Monitor IT infrastructure. DSS02.03 Verify, approve and fulfill service requests. DSS05.02 Manage network and connectivity security. DSS05.04 Manage user identity and logical access. DSS05.05 Manage physical access to IT assets. DSS05.07 Monitor the infrastructure for security-related events. DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.
PCI DSS 3.0 Requirement *2. Do not use vendor-supplied defaults for system passwords and other security parameter*
COBIT 5 Process APO01.08 Maintain compliance with policies and procedures APO03.02 Define reference architecture. BAI03.03 Develop solution components. BAI03.10 Maintain solutions. DSS04.08 Conduct post-resumption review. DSS05.03 Manage end-point security. DSS05.05 Manage physical access to IT assets. DSS05.07 Monitor the infrastructure for security-relatedevents

Protection of Cardholder Data

Cardholder data must be stored under protection and displayed only under certain conditions. Relevant requirements include data storage, deletion, encryption and masking (figure 4).

PCI DSS addresses encryption as well as essentials such as handling electronic keys. If data are transmitted (e.g., via the Internet, wireless networks, Global System for General Packet Radio Service [GPRS], Mobile Communications [GSM]), there is an increased risk that an attacker can eavesdrop and manipulate cardholder data. Where cardholder data are transmitted over open public networks, their encryption is required. The application of encryption, as specified, is one of many suggested methods to minimize this risk

Fig 4—Processes for Protection of Cardholder Data
PCI DSS 3.0 Requirement 3.*Protect stored cardholder data.*
COBIT 5 Process
APO01.06 Define information (data) and system ownership. APO01.08 Maintain compliance with policies and procedures. APO13.01 Establish and maintain an information security management system (ISMS). APO13.03 Monitor and review the ISMS. BAI08.02 Identify and classify sources of information. BAI08.05 Evaluate and retire information. BAI09.02 Manage critical assets. BAI09.03 Manage the asset life cycle. DSS01.01 Perform operational procedures. DSS04.08 Conduct postresumption review. DSS05.03 Manage end-point security. DSS05.04 Manage user identity and logical access. DSS05.05 Manage physical access to IT assets. DSS05.06 Manage sensitive documents and output devices. DSS06.04 Manage errors and exceptions. DSS06.05 Ensure traceability of information events and accountabilities.
PCI DSS 3.0 Requirement 4. *Encrypt transmission of cardholder data across open, public networks*
COBIT 5 Process APO11.02 Define and manage quality standards, practices and procedures. APO11.05 Integrate quality management into solutions for development and servicedelivery. BAI03.03 Develop solution components. DSS01.01 Perform operational procedures. DSS01.02 Manage outsourced IT services. DSS01.04 Manage the environment. DSS01.05 Manage facilities. DSS05.01 Protect against malware. DSS05.02 Manage network and connectivity security. DSS05.03 Manage end-point security. DSS05.06 Manage sensitive documents and output devices. DSS06.05 Ensure traceability of information events and accountabilities.

II. VULNERABILITY MANAGEMENT

Development and maintenance of systems and applications must be secure. This includes the prevention or removal of vulnerabilities that can be exploited by attackers to compromise or manipulate cardholder data. Regular installation of operating systems patches and applications must be done in addition to secure programming practices for developments.Proper testing ensures that vulnerabilities are identified. (See figure 5.)

In order to protect systems against malicious software ,use of antivirus software is required. It can be based on behavior-based and pattern-based detection techniques. Behavior-based detection techniques can identify malware on the basis of nonconventional behavior patterns and Pattern-based detection techniques detect viruses only after new virus patterns are updated to the antivirus software.

Fig 5—Processes for Vulnerability Management

PCI DSS 3.0 Requirement
5. Use and regularly update antivirus software or programs.
COBIT 5 Process
APO12.01 Collect data.
APO12.03 Maintain a risk profile.
DSS05.01 Protect against malware

PCI DSS 3.0 Requirement
6. Develop and maintain secure systems and applications.
COBIT 5 Process
APO12.02 Analyze risk.
APO12.04 Articulate risk.
BAI03.03 Develop solution components.
BAI03.05 Build solutions.
BAI03.07 Prepare for solution testing.
BAI03.08 Execute solution testing.
BAI03.10 Maintain solutions.
BAI06.01 Evaluate, prioritize and authorize change requests.
BAI06.02 Manage emergency changes.
BAI06.03 Track and report change status.
BAI06.04 Close and document the changes.
BAI06.01 Evaluate, prioritize and authorize change requests.
BAI07.01 Establish an implementation plan.
BAI07.04 Establish a test environment.
BAI07.05 Perform acceptance tests.
BAI07.06 Promote to production and manage releases.
DSS05.01 Protect against malware.

III. ACCESS CONTROL MEASURES

The access to cardholder data must be restricted based on roles as defined by the business need. According to need –to-know and least-privilege principles, only those persons authorized who need to access cardholder data for the purpose of business should be permitted access. This requires the implementation of authorization and control management, where each person can be assigned role-based access control [RBAC] (figure 6).

Only a person who can be successfully authenticated using a authentication method will be allowed to access a computer or system.For each person with system access, the assignment of exclusive identification is required.

Trespassers who gain entry to offices or data centers could steal, damage or manipulate media (such as diskettes, CDs and hard disks) or computer components. Media can include electronic media as well as paper.

Physical access to cardholder data must also be restricted .With physical access control and the visible wearing of badges, unauthorized persons can be distinguished from authorized users.

Fig 6—Processes for Access Control Measures

PCI DSS 3.0 Requirement
7. Restrict access to cardholder data by business need-to-know.

COBIT 5 Process
DSS05.04 Manage user identity and logical access.

PCI DSS 3.0 Requirement
8. Assign a unique ID to each person with computer access.

COBIT 5 Process
APO03.02 Define reference architecture.
APO07.01 Maintain adequate and appropriate staffing.

PCI DSS 3.0 Requirement
9. Restrict physical access to cardholder data.

COBIT 5 Process
APO01.06 Define information (data) and system ownership.
DSS05.04 Manage user identity and logical access.
DSS05.05 Manage physical access to IT assets.

IV. MONITORING AND TESTING OF NETWORKS

All access to network resources and cardholder data must be monitored , tracked and logged (fig 7). With protocols, unauthorized access can be traced and identified. The PCI DSS requires logging and recording of every access to cardholder data.

Security processes and systems need to be regularly tested which includes regular scanning for attack vectors and vulnerabilities. The threats must be recognized and removed before they can be ill-used by a would-be attacker.

Fig 7—Processes for Monitoring and Testing of Networks
PCI DSS 3.0 Requirement
10. *Track and monitor all access to networker sources and cardholder data.*
COBIT 5 Process
DSS01.01 Perform operational procedures.
DSS01.03 Monitor IT infrastructure.
DSS04.08 Conduct postresumption review.
DSS05.04 Manage user identity and logical access.
DSS05.05 Manage physical access to IT assets.
DSS05.06 Manage sensitive documents and output devices.
DSS05.07 Monitor the infrastructure for security-related events.
DSS06.04 Manage errors and exceptions.
DSS06.05 Ensure traceability of information events and accountabilities.
PCI DSS 3.0 Requirement
11. *Regularly test security systems andprocesses.*
COBIT 5 Process
APO03.02 Define reference architecture.
APO12.03 Maintain a risk profile.
APO12.01 Collect data.
DSS02.01 Define incident and service request classification schemes.
DSS05.07 Monitor the infrastructure for security-related events.
MEA01.02 Set performance and conformance targets.
MEA01.03 Collect and process performance and conformance data.
MEA01.04 Analyze and report performance.
MEA02.01 Monitor internal controls.
MEA02.02 Review business process control effectiveness.
MEA02.03 Perform control self-assessments.
MEA02.04 Identify and report control deficiencies

Information Security Policy

An information security policy must be prepared andregularly by organizations and informed to, and complied by, all employees (fig 8). It states requirements for information security to which all employees are bound. Topics in an information security policy include the statement of the PCI DSS requirements, the training for security awareness, theformation of an incident response plan and the observing of the security posture of service providers.

Fig 8—Processes for Information Security Policy
PCI DSS 3.0 Requirement
12. *Maintain a policy that addresses information security for all personnel.*
COBIT 5 Process
APO01.01 Define the organizational structure.
APO01.02 Establish roles and responsibilities.
APO01.03 Maintain the enablers of the management system.
APO01.05 Optimize the placement of the IT function.
APO01.06 Define information (data) and system ownership.
APO13.01 Establish and maintain an ISMS.

V. CONCLUSION

Organizations that store, process or transmit cardholder data or authentication data must comply with security requirements of PCI DSS. By using confluence of COBIT 5 enabling processes, these companies can also cover PCI DSS 3.0 security requirements. From another point of view, they can use the PCI DSS 3.0 security requirements to facilitate a COBIT 5 implementation and achieve objectives to optimize risk levels and resource use.

REFERENCES

[1]. Visa, "Compliance Validation Details for Merchants," 2012
[2]. PCI DSSC, Payment Card Industry (PCI) Data Security Standard—Requirements and Security Assessment Procedures, Version 3.0, 2013
[3]. PCI DSSC, "Payment Card Industry (PCI) Data Security Standard—Summary of Changes from PCI DSS Version 2.0 to 3.0," 2013
[4]. ISACA, COBIT 5: Enabling Processes, 2012