Cloud Card Compliance Checklist

An efficient tool for securing deployment Card Solutions on the Cloud

Hassan El Alloussi, Laila Fetjah, Abdelhak Chaichaa
Department of Mathematics and Computer Science
University Hassan II, Ain Chock, Faculty of Sciences
Casablanca, Morocco
e-mail: halloussi@gmail.com, l.fetjah@fsac.ac.ma, chaichaa@fsac.ac.ma

***Abstract*—The Payment Card Industry Data Security Standard (PCI-DSS) is a standard that aims to harmonize and strengthen the protection of Card Data in the whole lifecycle. Since its introduction, it has always been an efficient tool for controlling Card data on a platform deployed internally. In addition, it has been proved that this standard is among the best one for gauging data security, because it dictates a series of scrupulous controls and how they could be implemented. However, with the coming of the Cloud, the strategies have changed and the issues in protecting Card data become more complex. In this paper, we continue our previous work by developing a checklist that will be a reference for the Cloud tenant to control the security of Card data and information on the Cloud Computing. In the next steps, we will focus on evaluating this checklist on a real Cloud environment. Afterward, we work on recommending more requirements and controls that the norm PCI-DSS could adopt to be more efficient on Cloud and later we will develop a new Self-Assessment Questionnaire as a reference for Qualified Security Assessors (QSA) to check on the environment.**

Keywords-Cloud Computing; PCI-DSS; Card Industry; PCI-SSC; Cloud Computing Alliance (CSA); Cloud Controls Matrix (CCM)

I. INTRODUCTION

As the competition puts pressure on companies to increase productivity and decrease capital investments, solutions like distributed computing, that offer scalable systems with low fees, are attractive options for management to take in consideration. However, when you are responsible for the security of the access and the network, the idea of migrating everything to an environment that is not controlled and even owned, probably makes the decision more difficult.

Therefore, many banks and card transactions companies, which are attracted to outsourcing card solution outside their premises, encounter several obstacles, mainly related to security and data governance. The client has the responsibility to know where its data are and where it is going. This concept is the basis to data security, and plays a significant role in achieving and maintaining compliance with security norms, mainly the PCI-DSS [2].

Unfortunately, most of the requirements focus on the merchant’s ability to implement network access controls, data control, and insuring that the applications installed respect the security norms by periodically test their effectiveness. In addition, it may be difficult to do it and insufficient in a Cloud platform, where the infrastructure is outsourced [7].

In this paper, we continue our previous work [1] by developing a checklist that will be an efficient tool for banks and Card companies to control if the Cloud platform is ready to receive Card solutions or not. We based our contribution on two mains frameworks: Cloud Controls Matrix (CCM) [6] developed by Cloud Computing Alliance (CSA) and PCI-DSS.

In the next section, there is an explanation of the main advantages of the CCM [4] and its domains. Section III explains the choices of domains on what we focus on. Section IV details the matrix developed and the correspondent checklist for client that allow them to verify the effectiveness of the platform outsourced (we give an extract of the checklist in Table I). Section V brings a critical view to PCI-DSS standard insufficiency in Cloud computing. Finally, we draw a conclusion in Section VI.

II. THE CCM AND THE PCI-DSS

In [1], we have explained the main purpose of the norm PCI-DSS, its strength and its weaknesses linked to the cloud domain; the referential is rich but it is not adapted to the cloud environment.

The Cloud Security Alliance’s CCM is a rich source of cloud security best practices designed as a framework to provide fundamental security principles to cloud vendors and cloud customers. It provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 16 domains (latest version 3.0.1) [4]. This tool provides the holistic adherence to the vast and ever evolving landscape of global data privacy regulations and security standards.

The CCM serves as the basis for new industry standards and certifications. It is the first ever baseline control framework specifically designed for managing risk in the Cloud Supply Chain:

- Addressing the inter- and intra-organizational challenges of persistent information security by clearly delineating control ownership.
- Providing an anchor point and common language for balanced measurement of security and compliance postures.

ISBN: 978-1-61208-427-5

The PCI-DSS is a broadly accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. Therefore, it is not possible for a client to leverage the benefits of cloud systems without jeopardizing security, and mainly Card Data.

In this paper, we focus on creating for each topic on CCM list a matching PCI-DSS requirement in order to get a series of checklists on what the client could depend on to verify the trustworthiness of the Cloud before deciding to outsource.

III. THE DOMAINS OF APPLICATION

In our work, we focused on 4 main areas (domains) because they represent a basis for any tenant to check and control Cloud before deciding to outsource or not. Figure 1 shows the four domains, which are Network and Transport security, Data Security, Application and interface security, and Business Continuity management:

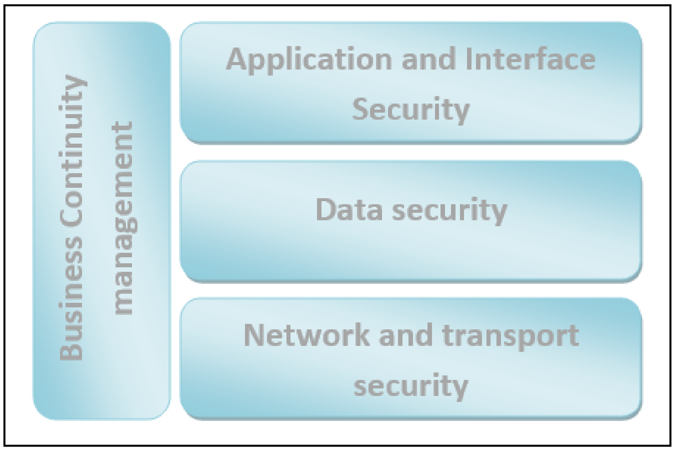
Business Continuity management
Application and Interface Security
Data security
Network and transport security

Figure 1. The domains developed in the checklist

- **Network and Transport security**: These controls allow verifying the security of the Card Data on network while it’s transmitted. It is essential for the tenant to check this aspect scrupulously before deploying on the Cloud.
- **Data Security**: These controls allow verifying the security of the Card data and preventing it from any leakage.
- **Application and interface security**: These controls aim to ensure that any Application and Programming Interface (APIs) is designed, developed, deployed and tested respecting the PCI-DSS norms in order to avoid any leakage.
- **Business Continuity management**: These controls aim at insuring the business continuity of the activities in any issue or disaster. The client should be sure that the activity could continue without any deterioration.

In the next section, we describe the checklist developed with an exhaustive questionnaire as a tool for any Cloud specialist to verify the compliance of a cloud and its readiness to outsource or not.

IV. THE CHECKLIST MATRIX

Our work, as described above, is developing a checklist based on 4 domains and 33 controls. Each control addresses a part of securing Transaction payment on the Cloud. In the first part, we describe each control and in the second one, we present a small extract of the Cloud Checklist. For the full and exhaustive Checklist, as the document size is limited, we suggest to refer to the authors.

A. Network security

1) Network Security (Infrastructure & Virtualization Security)

In this control, the auditor must ensure that:

- The Network environments and virtual instances are designed and are configured to restrict and monitor traffic between trusted and untrusted connections.
- The configurations of the Network are reviewed at least annually, and are supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.

2) Network Architecture (Infrastructure & Virtualization Security)

In this control, the auditor must ensure that:

- The network architecture diagrams have clearly identified high-risk environments and data flows that may have legal compliance impacts.
- The technical measures are implemented and apply defense-in-depth techniques for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.

3) VM Security - vMotion Data Protection (Infrastructure & Virtualization Security)

In this control, the auditor must ensure that:

- The secured and encrypted communication channels are used when migrating physical servers, applications, or data to virtualized servers
- There is a network segregation from production-level networks for such migrations.

4) Wireless Security (Infrastructure & Virtualization Security)

In this control, the auditor must ensure, in order to protect wireless network environments, that:

- There are policies and procedures that restrict the use of the this technology,
- The supporting business processes and technical measures are implemented.

5) Standardized Network Protocols (Interoperability & Portability)

In this control, the auditor must ensure that:

- The provider uses secure standardized network protocols for the import and export of data and to manage the service,

- The provider makes available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.

6) *Audit Logging / Intrusion Detection (Infrastructure & Virtualization Security)*

In this control, the auditor must ensure that:

- The provider is adhering to applicable legal, statutory or regulatory compliance obligations
- The provider is providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.

7) *Encryption (Encryption & Key Management)*

In this control, the auditor must ensure, for the use of encryption protocols for protection of sensitive data in storage and data in transmission, that:

- The Policies and procedures are established,
- The supporting business processes and technical measures are implemented, as per applicable legal, statutory, and regulatory compliance obligations.

8) *Antivirus / Malicious Software (Threat and Vulnerability Management)*

In this control, the auditor must ensure, in order to prevent the execution of malware on organizationally-owned or managed user end-point devices and IT infrastructure network and systems components, that:

- The policies and procedures are established.
- The supporting business processes and technical measures are implemented.

9) *Configuration Ports Access (Identity & Access Management)*

In this control, the auditor must ensure that the user access to diagnostic and configuration ports is restricted to authorized individuals and applications.

10) *Independent Audits (Audit Assurance & Compliance)*

In this control, the auditor must ensure that independent reviews and assessments are performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.

11) *User Access Policy (Identity & Access Management)*

In this control, the auditor must ensure, in order for ensuring appropriate identity, entitlement, and access management for internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components, that:

- The user access policies and procedures are established,
- The supporting business processes and technical measures are implemented.

12) *Segmentation (Infrastructure & Virtualization Security)*

In this control, the auditor must ensure that the Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, are designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users.

B. *Data Security & Information Lifecycle Management*

1) *Data Inventory / Flows*

In this control, the auditor must ensure that the policies and procedures are established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems (in particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds)

2) *Classification*

In this control, the auditor must ensure that data and objects containing data are assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.

3) *eCommerce Transactions*

In this control, the auditor must ensure that the data related to electronic commerce (e-commerce) that crosses public networks is appropriately classified, and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.

4) *Handling / Labeling / Security Policy*

In this control, the auditor must ensure that:

- The policies and procedures are established for labeling, handling, and the security of data and objects that contain data.
- The mechanisms for label inheritance are implemented for objects that act as aggregate containers for data.

5) *Nonproduction Data*

In this control, the auditor must ensure that the production data aren’t replicated or used in non-production environments.

6) *Ownership / Stewardship*

In this control, the auditor must ensure that all data is designated with stewardship, with assigned responsibilities defined, documented, and communicated.

7) *Secure Disposal*

In this control, the auditor must ensure that any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.

C. Application & Interface Security

1) Application Security

In this control, the auditor must ensure that the APIs are designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP [10] for web applications) and are adhered to applicable legal, statutory, or regulatory compliance obligations.

2) Customer Access Requirements

In this control, the auditor must ensure that prior to granting customer's access to data, assets, and information systems, all identified security, contractual, and regulatory requirements for customer access are addressed and are remediated.

3) Data Integrity

In this control, the auditor must ensure that the data input and output integrity routines (i.e., reconciliation and edit checks) are implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.

4) Data Security / Integrity

In this control, the auditor must ensure, in order to guarantee protection of confidentiality, integrity, and availability of data exchanged between one or more system interfaces, jurisdictions, or external business relationships to prevent improper disclosure, alteration, or destruction, that:

- The policies and procedures are established,
- The supporting business processes and technical measures are implemented.

D. Business Continuity Management & Operational Resilience

1) Business Continuity Planning

In this control, the auditor must ensure if all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements, that a consistent unified framework for business continuity planning and plan development is established, documented and adopted.

2) Business Continuity Testing

In this control, the auditor must ensure that:

- The business continuity and security incident response plans are subject to testing at planned intervals or upon significant organizational or environmental changes.
- The incident response plans involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

3) Datacenter Utilities / Environmental Conditions (Power / Telecommunications)

In this control, the auditor must ensure that datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) are secured, monitored, maintained, and tested for continual effectiveness at planned intervals.

4) Documentation

In this control, the auditor must ensure that information system documentation (e.g., administrator and user guides, and architecture diagrams) is made available to authorized personnel, in order to:

- Configure, install, and operate the information system,
- Effectively use the system's security features.

5) Environmental Risks

In this control, the auditor must ensure that the physical protection, against damage from natural causes and disasters, is anticipated, designed, and have countermeasures applied.

6) Equipment Location

In this control, the auditor must ensure, in order to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, that the equipment are kept away from locations subject to high probability environmental risks and are supplemented by redundant equipment located at a reasonable distance.

7) Equipment Maintenance

In this control, the auditor must ensure, for equipment maintenance ensuring continuity and availability of operations and support personnel, that:

- The policies and procedures are established,
- The supporting business processes and technical measures are implemented.

8) Policy

In this control, the auditor must ensure, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5), that:

- The policies and procedures are established,
- The supporting business processes and technical measures are implemented.

9) Retention Policy

In this control, the auditor must ensure, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations, that:

- The policies and procedures are established,
- The supporting business processes and technical measures are implemented.

In Table I, we illustrate an extract of the developed checklist. For each domain (from the main four described above), and for each sub-domain, we developed the questions that the auditors should verify and also how to verify the condition.

TABLE I. EXAMPLE OF CONTROL MATRIX (EXTRACT)

PCI-DSS Requirements Correspondent	Question	Expected Testing	In place	Not In Place	Reserves
A.1. Network Security					
PCI-DSS v3.0 1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Does a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks?	• Examine diagram(s) • Observe network configurations	□	□	□
	Is the network diagram kept updated?	• Interview responsible personnel	□	□	□
PCI-DSS v3.0 1.1.3 Current diagram that shows all cardholder data flows across systems and networks	Does the diagram show all cardholder data flows across systems and networks?	• Examine data-flow diagram • Interview personnel	□	□	□
	Is the diagram kept current and updated as needed upon changes to the environment?	• Examine data-flow diagram • Interview personnel	□	□	□
….	…	• …	□	□	□
A.7. Encryption					
PCI-DSS v3.0 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Were Encryption keys changed from default at installation?	• Interview responsible personnel • examine supporting documentation	□	□	□
	Are encryption keys changed anytime anyone with knowledge of the keys leaves the company or changes positions?	• Interview responsible personnel • examine supporting documentation	□	□	□
….	…	• …	□	□	□
A.9. Identity & Access Management: Configuration Ports Access					
PCI-DSS v3.0 1.2.2 Secure and synchronize router configuration files.	Are router configuration files secured from unauthorized access?	• Examine router configuration files	□	□	□
	Are router configurations synchronized?	• Examine router configurations	□	□	□
….	…	• …	□	□	□
B.3. eCommerce Transactions					
PCI-DSS v3.0 4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.)	Are end-user messaging technologies used to send cardholder data? (verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies)	• Observe processes for sending PAN • Examine a sample of outbound transmissions as they occur	□	□	□
	Is there a policy stating that unprotected PANs are not to be sent via end-user messaging technologies?	• Review written policies	□	□	□
….	…	• …	□	□	□
C.1. Application Security					
PCI-DSS v3.0 6.5 : Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop	Are developers required training in secure coding techniques based on industry best practices and guidance?	• Review policies and procedures for training • Interview personnel	□	□	□
	Are developers knowledgeable in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory?	• Interview personnel • Examine records of training	□	□	□

PCI-DSS Requirements Correspondent	**Question**	**Expected Testing**	**In place**	**Not In Place**	**Reserves**
applications based on secure coding guidelines.	Are processes to protect applications from the following vulnerabilities, in place?		□	□	□

V. Critical view to the standard PCI-DSS on the Cloud

Many controls specifications in the 4 domains treated above are not specified in any requirement in the recent version 3.0 of the PCI-DSS norm. These control specifications are:

- Network and Infrastructure Services: this control specification aims verifying that the Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, is designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.
- Equipment Power Failure: this control specification aims verifying Information security measures and redundancies are implemented to protect equipment from utility service outages (e.g. power failures and network disruptions).
- Impact Analysis: this control specification aims verifying that there is a defined and documented method for determining the impact of any disruption to the organization that must incorporate the following:
  - Identify critical products and services
  - Identify all dependencies, including processes, applications, business partners, and third party service providers
  - Understand threats to critical products and services
  - Determine impacts resulting from planned or unplanned disruptions and how these vary over time
  - Establish the maximum tolerable period for disruption
  - Establish priorities for recovery
  - Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption
  - Estimate the resources required for resumption.

In the next steps, we will evaluate this new framework by applying it on a real Card platform outsourced on the Cloud and we check its vulnerability and resilience. Afterward, we continue our work by focusing on developing recommended requirement for PCI-DSS for these control specification that could be added in the next update version of the norm.

VI. Conclusion and future work

The goal of the PCI-DSS is to protect cardholder data that is processed, stored or transmitted by providers, issuers or merchants. The security controls and processes required by PCI-DSS are vital for protecting cardholder account data. With all the advantages that give Cloud, Issuers, and Merchants and any other service providers involved with payment card processing must insure that the platform virtually and physically is sufficiently protected.

In this paper, we have developed an exhaustive checklist as a tool for any card stakeholder who wants to outsource a part or the whole card processing in a Cloud. In the next steps of our work, we will focus on evaluating the robustness of this framework by applying it on a real application of Card Transaction Platform on the Cloud environment. Afterward, we will develop recommended requirements for PCI-DSS necessary for the Cloud Environment and we will release a new Self-Assessment Questionnaire as a reference for a Qualified Security Assessor to check in the Cloud environment.

References

[1] H. El Alloussi, L. Fetjah, and A. Chaichaa, “Securing the Payment Card Data on Cloud environment: Issues & perspectives”, International Journal Of Computer Science and Network Security, Vol. 14, no. 11, Nov. 2014, pp. 14-20, http://paper.ijcsns.org/07_book/html/201411/201411003.html.

[2] PCI Security Standards Council, “Requirements and Security Assessment Procedures”, Version 3.0, November 2013, https://www.pcisecuritystandards.org [retrieved: May, 2015].

[3] PCI Security Standards Council, Summary of Changes from PCI-DSS Version 2.0 to 3.0”, November 2013, https://www.pcisecuritystandards.org [retrieved: May, 2015].

[4] Cloud Special Interest Group (PCI Security Standards Council), “PCI-DSS Cloud Computing Guidelines”, February 2013, https://www.pcisecuritystandards.org [retrieved: May, 2015].

[5] PCI Security Standards Council, “Payment Card Industry (PCI), Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS), Glossary of Terms, Abbreviations, and Acronyms”, Version 3.0, January 2014, https://www.pcisecuritystandards.org.

[6] Cloud Security Alliance (CSA), “CCM 3.0.1”, https://cloudsecurityalliance.org/research/ccm/ [retrieved: May, 2015].

[7] G. Ataya, “PCI-DSS audit and compliance”. In information security technical report 15 (2010) 138 -144.

[8] H. Rasheed, “Data and infrastructure security auditing in cloud computing”, In International Journal of Information Management 34 (2014) 364–368.

[9] W. Spangenberg, “PCI Compliance in the Cloud: What are the Risks?”, http://www.ioactive.com/pdfs/PCIComplianceInTheCloud.pdf.

[10] The Open Web Application Security Project (OWASP) Vulnerable Web Applications Directory Project, https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project, March 2015.

[11] G. Parann-Nissany, “Introduction to PCI-DSS and the Cloud”, Sep 2013, http://www.infoq.com/articles/cloud-pci-compliance.

[12] J. P. de Albuquerque and P. L. de Geus. “A Framework for Network Security System Design”, WSEAS Transactions on Systems, Piraeus,Greece, v. 2, n. Issue 1, 2003, p. 139-144.

[13] N. Carr, “The Big Switch: h: Rewiring the World, from Edison to Google”, W.W. Norton & Co., NY, 2008.

[14] A. Toffler, “The Third Wave”, Bantam (1980).

[15] The ISO 27000 Directory, http://www.27000.org/, [retrieved: May, 2015].

[16] ISACA Global Organization/ COBIT, http://isaca.org/cobit.

[17] The National Institute of Standards and Technology, http://www.nist.gov/, [retrieved: May, 2015].

[18] The Technology Policy Division of the Financial Services Roundtable, http://www.bits.org, [retrieved: May, 2015].

[19] Generally Accepted Privacy Principles, https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/, [retrieved: May, 2015].

[20] Health Insurance Portability and Accountability Act (HIPAA), http://www.ohii.ca.gov/calohi/PrivacySecurity/HIPAA.aspx, [retrieved: May, 2015].

[21] Jericho Forum, http://www.jerichoforum.org, [retrieved: May, 2015].

[22] North American Electric Reliability Corporation- Critical infrastructure protection, http://www.nerc.com/, [retrieved: May, 2015].