Securing Card data on the Cloud

Application of the Cloud Card Compliance Checklist

Hassan El Alloussi, Laila Fetjah, Abdelhak Chaichaa
Department of Mathematics and Computer Science
Faculty of Sciences Aïn Chock
Hassan II University of Casablanca, P.O Box 5366
Casablanca, Morocco
e-mail: halloussi@gmail.com, l.fetjah@fsac.ac.ma, chaichaa@fsac.ac.ma

***Abstract*—Cloud Computing did come up with so many attractive advantages such as scalability, flexibility, accessibility, rapid application deployment, user self-service and mainly cost effectiveness. However, security issues and lack of governance let users hesitating before deciding. In the other side, with the advent of many means of payment, other than coins and banknotes, the security is also the big issue. Many tools has been developed to help Card Industry stakeholder to develop their products with minimal concern, like Payment Card Industry Data Security Standard. In fact, the Payment Card Industry Data Security Standard 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 work on 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. Also, we will evaluate our result by applying our checklist on a real Cloud environment. In next steps, we will focus on evaluating Risk Management of deployed Card Transaction Platform on a Public Cloud and all the strategies to reduce impacts of all potential risks.**

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

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, developed in [1], 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 [3].

In this paper, we will expose our complete work by developing our methodology to get an exhaustive tool for auditing 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. Also, we illustrate our work by a real use case. We based our contribution on two mains frameworks: Cloud Controls Matrix (CCM) [4] developed by Cloud Computing Alliance (CSA) and PCI-DSS.

In the next section, we illustrate some basic aspects of the Cloud Computing and the Card Payment Industry. In Section III, we explain the main advantages of the CCM [4] and its domains. Section IV explains the choices of domains on what we focus on. Section V 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 IV). Section V brings a critical view to PCI-DSS standard insufficiency in Cloud computing. A use case is illustrated in Section VII. And finally, we draw a conclusion in Section VIII.

II. BACKGROUND

As mentioned before, in this section we explain the basics aspects; Cloud Computing, The Payment Industry, the CSA and the PCI-DSS.

A. Cloud Computing: the new opportunity

Cloud Computing means outsourcing your data and its processing on remote servers, which eliminates the need to store these on premises. The interest is to access that data from any Internet-connected computer and synchronization across multiple devices.

The benefits are many; including a gain of space, resources, time and money. The user can freely access documents without worrying about the machine he uses. Cloud computing is, essentially, an economic commercial offer subscription to external services.

However, to adopt the Cloud, the customer should manage security issues, including legal and contractual aspects. Indeed, the advent of cloud computing brings new solutions to significant improvement in security. The data are stored in the cloud and should be always accessible no matter what happens to all access devices (laptop, Tablet, Smartphone, etc.).

B. Payment Card Industry: The evolution

Electronic payment means all electronic flows of information and treatment needed to manage credit cards and associated transactions. Electronic money transfers have been conducted by banks since the 1960's and bank customers have been able to draw cash from ATM's since the 1970's (NCR, Diebold, Wincor, etc.).

Historically, the first credit Cards, were existed before 1970, and were equipped with only "Embossing" (i.e., customer data printed in relief on the physical media). Information is the number of the card (backed by a bank account), the name and surname of the owner, date of expiry, etc.

In the mid-90s, electronic banking has evolved to include a new fully electronic channel and e-Commerce, which is buying and selling of products or services via the web, Internet or other computer networks while M-commerce (or mobile commerce) is the buying of products or services via a device like Smartphone, PDA, etc.

1) The stakeholders involved with payment card transactions:

- **Card holder**: a person holding a payment card (the consumer in B2C).
- **Merchant**: the business organization selling the goods and services (The merchant sets up a contract known as a merchant account with an acquirer).
- **Service provider**: this could be the merchant itself (Merchant service provider (MSP)) or an independent sales organization providing some or all of the payment services for the merchant.
- **Acquirer or acquiring bank**: this connects to a card brand network for payment processing and also has a contract for payment services with a merchant.
- **Issuing bank**: this entity issues the payment cards to the payment card holders.
- **Card brand**: this is a payment system (called association network) with its own processors and acquirers (such as Visa, MasterCard or CMI card in Morocco).

In Figure 1, we illustrate the relation between the stakeholders in Card Payment.

Figure 1. Payment card stakeholders

2) Payment cards flowchart:

Basically payment cards work using two components (Figure 2). The first one, the 'transaction authorization', is where a message containing the transaction details is sent to the card issuer requesting authorization for the payment. The card issuer then authorizes the payment. This guarantees payment to the merchant.

The second component known as 'clearing' is where the merchant submits the authorized transaction for payment (automatically or manually; daily or periodically) to Service Provider. The transaction then appears in the card holder's statement.

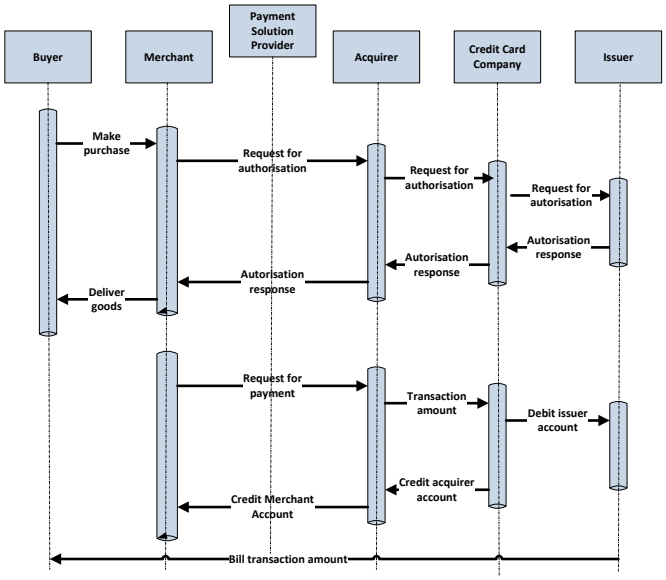

Figure 2. Payment Card Flowchart

However, in e-commerce/m-commerce, the payment methods are slightly different.

3) The e-commerce/m-commerce system model

Generally, most e-commerce/m-commerce systems can be designed as a three tier model. The three component parts are the client side, the service system and the back end

system. These two last components are commonly known as 'Server Side'.

The client side connects users to the Server Side, which deals the users' requests. From a business perspective the client side provides the customer interface, the service system provides the business logic and the back-end provides the required data to complete a transaction to its fate.

E-commerce/m-commerce system vulnerabilities

The transaction process highlights the requirement for communication between the users, merchant, card issuer and may be the service provider. These communications must be protected to ensure confidentiality and integrity of the transaction details. This will prevent spying and data manipulation of the transaction details.

By understanding the e-commerce/m-commerce system architecture it becomes apparent that the payment card data will be vulnerable if someone having obtained the payment card information details or can access the component parts of the server side system. Additionally, the communications between the component parts of the server side must be protected to ensure confidentiality and integrity of the transaction details.

C. The CSA: Cloud Security Alliance

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. It is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

The Cloud Security Alliance has designed many tools to manage control and governance on Cloud. Its main tool is Cloud Controls Matrix (CCM), which aims to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Cloud Control Matrix: a reliable tool to assess security risk of Cloud environment

The Cloud Security Alliance's Cloud Controls Matrix 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):

1. Application & Interface Security
2. Audit Assurance & Compliance
3. Business Continuity Management & Operational Resilience
4. Change Control & Configuration Management
5. Data Security & Information Lifecycle Management
6. Datacenter Security
7. Encryption & Key Management
8. Governance and Risk Management
9. Human Resources
10. Identity & Access Management
11. Infrastructure & Virtualization Security
12. Interoperability & Portability
13. Mobile Security
14. Security Incident Management, E-Discovery & Cloud Forensics
15. Supply Chain Management, Transparency and Accountability
16. Threat and Vulnerability Management

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.
- Providing the holistic adherence to the vast and ever evolving landscape of global data privacy regulations and security standards.

The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will provide internal control direction for service organization control reports attestations provided by cloud providers. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. The CSA CCM strengthens existing information security control environments by emphasizing business information security control requirements, reduces and identifies consistent security threats and vulnerabilities in the cloud, provides standardized security and operational risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

PCI DSS [6]: is an industry wide set of requirements that affects any company or organization that accepts, processes, transmits or stores card details or any sensitive data linked to the payment card. It aims to encourage merchants and service providers to protect payment card data. This ultimately leads to the reduction of fraud losses for banks, merchants and card brands.

ISO 27001/27002 [7]: are the best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), published jointly by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). While ISO27017 and ISO27018 are respectively for Information security management for cloud systems and Data protection for cloud systems are as draft now, the main framework still now ISO 27001/27002.

ISO 27001 is an internationally accepted standard framework for an information security management system that includes control requirements in 11 domains. Those that

do implement ISO 27001 may further choose to have their compliance independently audited to obtain ISO 27001 certification.

ISACA COBIT [8]: is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. It aims to research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals. The benefits that frameworks such as COBIT offer is that they produce a summary assessment of the business risks and achieved business value of an application, and they can help practitioners evaluate (often to a highly granular degree) many security or value issues.

NIST [9]: The National Institute of Standards and Technology (NIST) has been designated by the Federal Chief Information Officer (CIO) to accelerate the federal government's secure adoption of cloud computing by leading efforts to identify existing standards and guidelines.

BITS [10]: stands for "Banking Industry Technology Secretariat, however a BITS Shared Assessment provides an assessment of an organization's implementation of its controls using a standardized questionnaire, which is based on the ISO 27002 standard, with additional input from Shared Assessments Program members. The approach is more rigidly defined (e.g., answers are Yes, No, or N/A, making the completed SIG easy to read by machine. The original idea was that service providers could complete the SIG just once, and then provide the completed SIG to multiple clients.

In short, the BITS Shared Assessment cost is a little more and is a little less flexible – but it provides a higher level of interim attestation in return.

GAPP (Generally Accepted Privacy Principles) [11]: are privacy principles and criteria developed and updated by the AICPA and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.

HIPAA/HITECH (Health Insurance Portability and Accountability Act) [12]: The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Jericho Forum [13]: is an international group of organizations working together to define and promote the solutions surrounding the issue of de-perimeterisation. It was officially founded at the offices of the Open Group in Reading, UK, on Friday 16 January 2004. It had existed as a loose affiliation of interested corporate CISOs (Chief Information Security Officers) discussing the topic since the summer of 2003.

NERC CIP (North American Electric Reliability Corporation- Critical infrastructure protection) [14]: is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation.

In our work, we focus firstly on PCI DSS framework to provide a questionnaire to control card data on the cloud and give a critical review to improve the framework and add more requirements for Cloud Computing. Afterward, we extend the work to the other frameworks in order to have a complete checklist a standard for Cloud Computing adopters

D. The PCI DSS

The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

The Council's five founding global payment brands - American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc - have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs (Qualified Security Assessors) PA-QSAs (Payment application Qualified Security Assessors) and ASVs (Approved Scanning Vendor) certified by the PCI Security Standards Council.

1) What are the PCI DSS requirements?

PCI DSS is a set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks.

The PCI DSS specifies and elaborates on six major objectives and twelve requirements (Table I).

These requirements are intended to reduce the risk of transactions and promote a holistic approach to the security of the Card Data Environment (CDE). It is important for companies to understand the scope of PCI DSS and how to implement the controls to meet the requirements.

TABLE I. THE PCI-DSS REQUIREMENTS

Activities	Describing the 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 defaults for system passwords and other security parameters.
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 test security systems and processes
Maintain an Information security policy.	12. Maintain a policy that addresses information security for all personnel

2) PCI DSS compliance in Cloud environments:

PCI DSS, as stated earlier in this section, applies to any company or organization that accepts, processes, transmits or stores payment card details or any sensitive data associated with a payment card. Merchants and service providers must comply with the all the requirements regardless of their size and how many transactions they process.

On February 2013 PCI DSS Cloud Computing Guidelines state, The responsibilities delineated between the client and the Cloud Service Provider (CSP) for managing PCI DSS controls are influenced by a number of variables, including but not limited to:

- The purpose for which the client is using the cloud service
- The scope of PCI DSS requirements that the client is outsourcing to the CSP
- The services and system components that the CSP has validated within its own operations
- The service option that the client has selected to engage the CSP (IaaS, PaaS or SaaS)
- The scope of any additional services the CSP is providing to proactively manage the client's compliance (for example, additional managed security services)

Hereafter, we show, in Table II, an example of how the responsibilities are sharing following the Cloud Layers.

TABLE II. RESPONSIBILITIES SHARING ON CLOUD LAYERS

	Client
	CSP

Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data			
Interface (APIs, GUIs)			
Application			
Solution Stack (Programming languages)			
Operating Systems (OS)			
Virtual Machines			
Virtual network infrastructure			
Hypervisors			
Processing and memory			
Data Storage (hard drives, removable disks, backups, etc)			
Network (Interfaces and devices, communications			
Physical facilities / data centers			

Also, we show, in Table III, how the responsibilities are sharing following PCI DSS Requirements.

TABLE III. RESPONSIBILITIES SHARING ON PCI DSS REQUIREMENT

	Client
	CSP
	Both Client and CSP

PCI DSS Requirement	Service Models		
	IaaS	PaaS	SaaS
1. Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2. Do not use vendor supplied defaults for system passwords and other security parameters.	Both	Both	CSP
3. Protect stored cardholder data	Both	Both	CSP
4. Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5. Protect all systems against malware and regularly update anti-virus software or programs	Client	Both	CSP
6. Develop and maintain secure systems and applications	Both	Both	Both
7. Restrict access to cardholder data by business need to know	Both	Both	Both
8. Identify and authenticate access to system components	Both	Both	Both

9. Restrict physical access to cardholder data	CSP	CSP	CSP
10. Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11. Regularly test security systems and processes	Both	Both	CSP
12. Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

3) Considerations in managing PCI DSS on the Cloud computing:

a) Segmentation of the Cloud:

a. Segmentation on a cloud-computing infrastructure must provide an equivalent level of isolation as that achievable through physical network separation
b. Other client environments running on the same infrastructure are to be considered untrusted networks
c. The CSP needs to take ownership of the segmentation between clients
d. The client is responsible for the proper configuration of any segmentation controls implemented within their own environment

b) Recommendations for Reducing Scope:

a. Do not store, process or transmit payment card data in the cloud
b. Implement a dedicated physical infrastructure that is used only for the in-scope cloud environment
c. Minimize reliance on third-party CSPs for protecting payment card data
d. It can be challenging to verify who has access to cardholder data processed, transmitted, or stored in the cloud environment
e. It can be challenging to collect, correlate, and/or archive all of the logs necessary to meet applicable PCI DSS requirements
f. Organizations using data-discovery tools to identify cardholder data in their environments, and to ensure that such data is not stored in unexpected places, may find that running such tools in a cloud environment can be difficult and result in incomplete results.

Many large providers might not support right-to-audit for their clients. Clients should discuss their needs with the provider to determine how the CSP can provide assurance that required controls are in place

III. THE CCM AND THE PCI-DSS: THE STATE OF THE ART

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) [6]. 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.

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 our work, 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.

IV. 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 3 shows the four domains, which are Network and Transport security, Data Security, Application and interface security, and Business Continuity management.

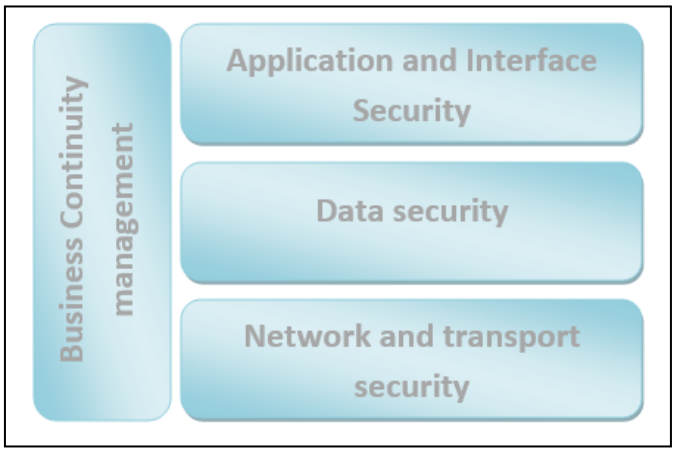

Figure 3. The domains developed in the checklist

- **Network and Transport security**: These controls allow verifying the security of the Card Data on network while it is 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.

V. THE CHECKLIST MATRIX

Our work, as described above, is developing a checklist based on 4 domains and 32 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 are not 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 [19] 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 IV, 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 IV. 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	☐	☐	☐
…	…	• …	☐	☐	☐

PCI-DSS Requirements Correspondent	Question	Expected Testing	In place	Not In Place	Reserves
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 applications based on secure coding guidelines.	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	☐	☐	☐
	Are processes to protect applications from the following vulnerabilities, in place?		☐	☐	☐
D.7. Equipment Maintenance					
PCI DSS v3.0 10.8 Ensure that security policies and operational	Are security policies and operational pro-cedures for	• Examine documentation • Interview	☐	✓	☐
procedures for monitoring all access to net-work resources and cardholder data are documented, in use, and known to all affected par-ties.	monitoring all access to net-work resources and cardholder data docu-mented, In use, and Known to all affected parties?	personnel			

VI. 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 step, we will evaluate, as a use case, 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.

VII. USE CASE

In this section, we describe how we applied the framework on a Card Transaction Platform developed as part of this project. Firstly, we will describe the solution HibaPay, its functionalities and its architecture. Afterward, we will apply the framework checklist and we will describe the result on the platform.

However, the solution HibaPay is deployed in a public Cloud and it is ready for processing.

A. Card Data Processins Solution on Cloud

HibaPay is an electronic Card Transaction Platform that allows banks to convert the opportunities offered by the development of smartphones and increase in revenue by setting up financial services that are simple and powerful.

The design of the platform HibaPay considers integrated manner the interests and constraints of the various stakeholders: the Client, the Merchant and the Bank. It also includes a prospective view of the state of the art either in the world of Mobile Phones or that of Electronic Card payment.

The platform HibaPay allows banks and operators to explore all business development opportunities offered by the financial Solutions in meeting with the specific needs of each market. HibaPay includes modules able to realize synergies between market players of mobile financial services.

In Figure 4, we illustrate the architecture of the solution HibaPay.

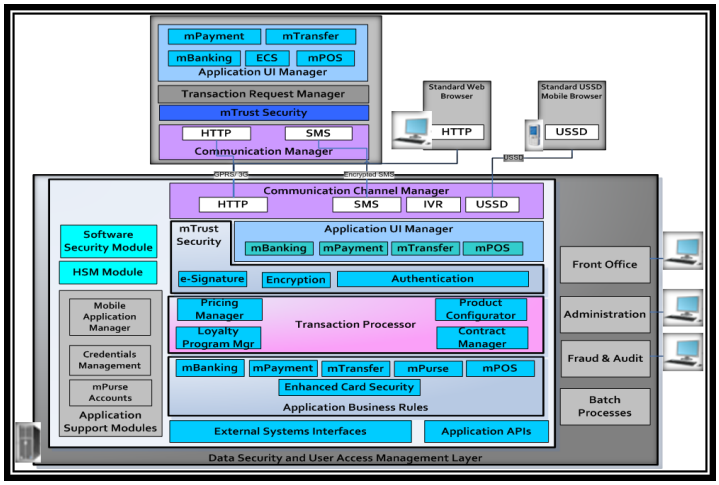

Figure 4. The Card Processing Solution Architecture

The HibaPay main modules are:

The server Modules:

- mTrust Security
- Software Security Module
- Transaction Manager
- Credentials Manager
- Applications UI Manager
- Communication Channels Manager
- Mobile Application Manager
- mPurse Accounts Manager

The application Modules:

- mBanking
- mPayment
- mTransfer
- mPurse
- mPoS
- Enhanced Card Security

B. Appraisal

Once we deployed the solution, we audit the solution and we illustrate in Table V an extract of the result.

TABLE V. SAMPLE OF THE AUDIT RESULT

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	☐	☐	√
….	…	• …	☐	☐	☐
B.3. eCommerce Transactions					
PCI-DSS v3.0 4.2 Never send	Are end-user messaging	• Observe	√	☐	☐

PCI-DSS Requirements Correspondent	Question	Expected Testing	In place	Not In Place	Reserves
unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.)	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)	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 applications based on secure coding guidelines.	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	☐	☐	✓
	Are processes to protect applications from the following vulnerabilities, in place?		☐	☐	☐
D.7. Equipment Maintenance					
PCI DSS v3.0 10.8 Ensure that security policies and operational procedures for monitoring all access to net-work resources and	Are security policies and operational procedures for monitoring all access to network resources and cardholder	• Examine documentation • Interview personnel	☐	✓	☐
cardholder data are documented, in use, and known to all affected par-ties.	data documented, In use, and Known to all affected parties?				
PCI DSS v3.0 11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Are security policies and operational procedures for security monitoring and testing documented, in use, and known to all affected parties?	• Examine documentation • Interview personnel	✓	☐	☐

C. Analysis

In our audit of the platform, we stated that many requirements are not in place or there are reserves. So, many actions must be in place to remove these differences.

For example, in the "Network Security", we noted a reserve on "Cloud Provider" (see Table VI).

TABLE VI. SAMPLE OF AUDIT RESULT WITH "RESERVES"

PCI-DSS Requirements Correspondent	Question	Expected Testing	In place	Not In Place	Reserves
A.1. Network Security					
PCI-DSS v3.0 1.1.3 Current diagram that shows all cardholder data flows across systems and networks	Is the diagram kept current and updated as needed upon changes to the environment?	• Examine data-flow diagram • Interview personnel	☐	☐	✓

Indeed, after auditing, we found that the cloud provider does not update the network diagram after a change on environment. For this, we asked to add a firewall to improve access security. However, we found that the chart was not updated in time.

Another example, Table VII, we found during the audit that security policies and operational procedures for monitoring all access to network resources and cardholder data documented are not known by the provider staff Cloud. For this, training must be established to prepare the personnel of Cloud Provider for the types of data they will handle.

TABLE VII. SAMPLE OF AUDIT RESULT WITH REQUIREMENT "NOT IN PLACE"

PCI-DSS Requirements Correspondent	Question	Expected Testing	In place	Not In Place	Reserves
D.7. Equipment Maintenance					
PCI DSS v3.0 10.8 Ensure that security policies and operational procedures for monitoring all access to net-work resources and cardholder data are documented, in use, and known to all affected par-ties.	Are security policies and operational pro-cedures for monitoring all access to net-work resources and cardholder data docu-mented, In use, and Known to all affected parties?	• Examine documentation • Interview personnel	☐	√	☐

In the next steps, in order to prepare a successful deployment, we monitor the implementation of all necessaries actions to eliminate all reserves and implementing all the requirement, which are not "In place".

VIII. 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 the work, we will focus evaluating Risk Management of deployed Card Transaction Platform on a Public Cloud and all the strategies to reduce impacts of all potential risks.

REFERENCES

[1] H. El Alloussi, L. Fetjah, and A. Chaichaa, "Cloud Card Compliance Checklist : An Efficient Tool for Securing Deployment Card Solutions on the Cloud," IARIA SECURWARE 2015 : The Ninth International Conference on Emerging Security, ISBN: 978-1-61208-427-5 98, August 2015, pp. 98-104.

[2] PCI Security Standards Council, "Requirements and Security Assessment Procedures," Version 3.1, May 2015, https://www.pcisecuritystandards.org [retrieved: May, 2016].

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

[4] Cloud Security Alliance (CSA), "CCM 3.0.1," https://cloudsecurityalliance.org/research/ccm/ [retrieved: May, 2016].

[5] 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.

[6] PCI Security Standards Council, Summary of Changes from PCI DSS Version 3.0 to 3.1," April 2015, https://www.pcisecuritystandards.org [retrieved: May, 2016].

[7] The ISO 27000 Directory, http://www.27000.org/, [retrieved: May, 2016].

[8] ISACA Global Organization/ COBIT, http://isaca.org/cobit, [retrieved: May, 2016].

[9] The National Institute of Standards and Technology, http://www.nist.gov/, [retrieved: May, 2016].

[10] The Technology Policy Division of the Financial Services Roundtable, http://www.bits.org, [retrieved: May, 2016].

[11] Generally Accepted Privacy Principles, https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/, [retrieved: May, 2016].

[12] Health Insurance Portability and Accountability Act (HIPAA), http://www.ohii.ca.gov/calohi/PrivacySecurity/HIPAA.aspx, [retrieved: May, 2016].

[13] Jericho Forum, http://www.jerichoforum.org, [retrieved: May, 2016].

[14] North American Electric Reliability Corporation- Critical infrastructure protection, http://www.nerc.com/, [retrieved: May, 2016].

[15] Cloud Special Interest Group (PCI Security Standards Council), "PCI-DSS Cloud Computing Guidelines," February 2013, https://www.pcisecuritystandards.org [retrieved: May, 2016].

[16] 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 [retrieved: May, 2016].

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

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

[19] The Open Web Application Security Project (OWASP) Vulnerable Web Applications Directory Project, https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project [retrieved: May, 2016].

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

[21] J. P. de Albuquerque and P. L. de Geus. "A Framework for Network Security System Design," WSEAS Transactions on Systems, Piraeus,Greece, vol. 2, no. 1, 2003, pp. 139-144.

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

[23] A. Toffler, "The Third Wave," Bantam (1980).