Securing the Payment Card Data on Cloud environment: Issues & perspectives

Hassan EL ALLOUSSI, Laila FETJAH, Abdelhak CHAICHAA

Department of Mathematics and Computer Science University Hassan II, Ain Chock, Faculty of Sciences P.O Box 5366, Mâarif – Casablanca, Morocco

Summary

Cloud computing is a new IT model that, just like electricity and water, which were firstly generated at home and evolved to be supplied from utility providers, aims to transform computing resources sharing into an utility. This enables startups and other companies to start computing services without having to invest directly in dedicated infrastructure (Moving from CAPEX to OPEX). However, many security challenges has to be overcame by stakeholders (providers and tenants) to ensure that the customer's data are safe and secured. Many security norms and frameworks have been focused on new security challenges on Cloud. So, organizations involved in payment card processing including those that store, process, or transmit credit cardholder data are required by credit card companies to implement The Payment Card Industry (PCI) Data Security Standard (DSS). In this paper we describe the advantages and security challenges in outsourcing data in Cloud Computing, giving criticism to security frameworks, and focusing, on the next steps on developing a checklist using standard frameworks.

Keywords:

Cloud computing, Computer architecture, PCI DSS, Card, Card Industry, ISO27001, ISO27002, Visa, Mastercard, PCI SSC, Qualified Security Assessor.

1. Introduction

Nowadays, Cloud Computing is commercialized as the perfect solution to the majority of an organization's IT needs. Combining this with the growth of Card payment transactions volume, it became necessary for organizations to use a cloud service's flexibility to meet its business requirements. However, before moving IT services to the cloud, an organization must consider the contractual, legal, regulatory obligations, and security and integrity disposition it has to protect its data. The Payment Card Industry Data Security Standard (PCI DSS) was created to protect cardholder data. In this paper, we provide the definitions of what cloud computing actually is and the services offered, a summary of two services providers cloud services and a review of what the Payment Card Industry Security Standards Council's concerns regarding virtualization and Cloud environment. By understanding the architecture of Payment Card solutions and the controls available within virtualization and hardware technologies, it has been possible to conclude that PCI DSS compliance is achievable within a cloud hosted environment, but under a special control.

Hereafter, in section II, we describe the Cloud Computing, what companies lose when they don't adopt it. In section III, we focus on describing Card payment evolution and its challenges in the Cloud environment. In section IV, we define the Cloud Security Alliance objectives and mainly the development of its matrix for controlling security in Cloud computing. In section V, we focus on PCI-DSS framework and the new challenges they have with the Cloud Era.

2. The Cloud Computing: The loss in non adoption

Cloud Computing means outsourcing your data 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 oversee 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…).

The road to Cloud Computing era

To understand what is cloud computing, it is important to understand how this model of computing has evolved. In his famous book, The Third Wave (Bantam, 1980), Alvin Toffler notes that civilization has progressed in waves (three of them to date: the first wave was agricultural

Manuscript received November 5, 2014
Manuscript revised November 20, 2014

societies, the second was the industrial age, and the third is the information age).

Within each wave, there have been several important subwaves. In this post-industrial information age, we are now at the beginning of what many people feel will be an era of cloud computing.

Also, Nicholas Carr discusses, in his book The Big Switch (W.W. Norton & Co., 2008), an information revolution very similar to an important change within the industrial era. Particularly, Carr equates the rise of cloud computing in the information age to electrification in the industrial age. It used to be that organizations had to provide their own power (ex. water wheels, windmills).

With electrification, however, organizations no longer provide their own power; they just plug in to the electrical grid. Carr argues that cloud computing is really the beginning of the same change for information technology. Now organizations provide their own computing resources (power). The emerging future, however, is one in which organizations will simply plug in to the cloud (computing grid) for the computing resources they need. As he puts it, “In the end the savings offered by utilities become too compelling to resist, even for the largest enterprises.

Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being announced regularly.

3. 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…).

Historically, the first credit Cards, were existed before 1970, and were equipped with only "Embossing" (ie 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.

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).

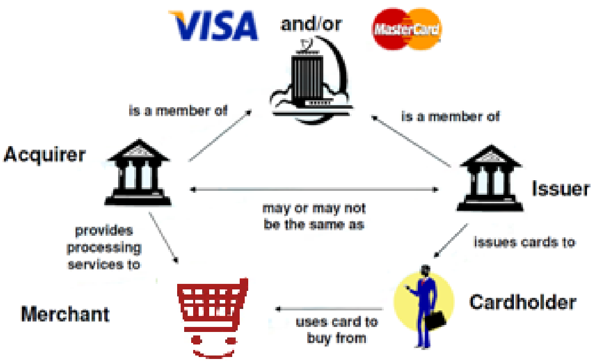

Figure 1: Payment card stakeholders

Payment cards flowchart:

Basically payment cards work using two components. 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.

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

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.

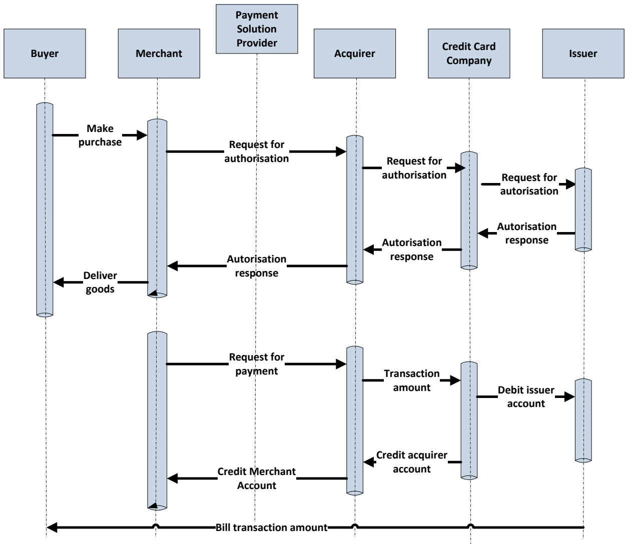

Figure 2: Payment Card Flowchart

4. 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.

- ***ISO 27001/27002 [13]*** : 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 [14]***: 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.

- ***PCI DSS [2]***: 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.

- ***NIST [15]***: 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 [16]***: 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) [16]***: 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) [18]***: 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***: 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) [20]***: 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.

5. PCI DSS: Payment Card Industry – Data Security Standards

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.

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:

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

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.

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 an example of how the responsibilities are sharing following the 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	🟩	🟩	🟩

Figure 3: Responsibilities sharing on Cloud Layers

Also, we show how the responsibilities are sharing following PCI DSS Requirements:

🟧	*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

Figure4: Responsibilities sharing on PCI DSS Requirement

Considerations in managing PCI DSS on the Cloud computing:

1. 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
2. Recommendations for Reducing Scope:
   a. Don't 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
   g. 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

6. Conclusion

As stated in earlier, Card transactions are exponentially increasing to become the world's most popular means of payment. The advent of Cloud Computing, and benefits that offer, has pushed many company to outsource their data processing and storing. So, many vulnerabilities have been detected and it was necessary for the CSP and the client to develop a methodology and a referential to help working together in order to enhance the security level.

The scope of the Cardholder Data Environment (CDE) for some organizations will be far greater than that of a merchant trying to sell products and services via a website. The solution for moving a supermarket CDE to a cloud environment would be very different to that of a merchant's e-commerce website.

However, with a correctly configured host system and CDE it would be possible to achieve PCI DSS compliance in a cloud environment. This would be on the condition that the cloud service was specifically developed to host PCI DSS compliant systems.

As detailed in this document, a Cloud Matrix Control could provide tools needed to comply with the PCI DSS. In the next step, we will develop a checklist to control card data on the cloud and giving a critical to improve the framework to add more requirements for Cloud Computing.

References

[1] PCI Security Standards Council, “Requirements and Security Assessment Procedures”, Version 3.0, Novembre 2013, https://www.pcisecuritystandards.org.

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

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

[4] 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.

[5] Cloud Security Alliance (CSA), “Cloud Controls Matrix 3.0.1”, https://cloudsecurityalliance.org/research/ccm/ .

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

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

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

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

[10] João Porto de Albuquerque, Paulo Lìcio de Geus. “A Framework for Network Security System Design”, WSEAS Transactions on Systems, Piraeus,Greece, v. 2, n. Issue 1, p. 139-144, 2003

[11] Alvin Toffler, “The Third Wave”, Bantam (1980)

[12] Nicholas Carr discusses, “The Big Switch”, W.W. Norton & Co. (2008)

[13] The ISO 27000 Directory, http://www.27000.org/

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

[15] The National Institute of Standards and Technology, http://www.nist.gov/

[16] The Technology Policy Division of the Financial Services Roundtable, http://www.bits.org

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

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

[19] Jericho Forum, http://www.jerichoforum.org

[20] North American Electric Reliability Corporation- Critical infrastructure protection, http://www.nerc.com/