Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Simple Prototype for Implementing PCI DSS by Using ISO 27001 Frameworks

[1]Abhishek Srivastav*, [2]Irman Ali, [3]Neeraj Kumar, [4]Ravi Shanker
[1,2,3,4]M.S. in Cyber Law & Information Security, India
[1,2,3,4]Indian Institute of Information Technology, Jhalwa, Allahabad, India

Abstract: ***Now a day's Information play a very importance role in any business. Primary concern in businesses today is to protect the information and critical data. We find a number of Laws, regulations, and standards are available that address the various issues of security. The Payment Card Industry has their own standards for the protection of customer critical information. PCI DSS not only become a very important standard for the protection of sensitive and confidential data but also it covers data that pertains to cardholder information. To comply with internationally recognized certificate, a lot of work along with a lot of resources needed. A very popular and probably the most important security certificate is ISO 27001. All merchants and service providers of e-commerce and card payment service need to be compliant with PCI DSS. In this paper we will show a model of how to reduce required resources and how to simplify achieving PCI DSS compliance by using ISO 27001.***

Keywords: Information Security, ISO 27001, PCI DSS, Compliance.

1 Introduction

Information Security is a much wide concept than technology. It concern with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. As the size of information grows, stored and communicated in electronic form, Information Security is rapidly becoming intertwined with technology, and more specifically, the internet. This has given rise to the term Cyber Security and for it to be used interchangeably with Information Security [1].

Electronic commerce, generally known as e-commerce, where the buying and selling of products or services is conducted over electronic systems such as the Internet and other computer networks [5]. E-commerce is generally considered to be the sales aspect of e-business. It also consists of the exchange of data to facilitate the financing and payment aspects of business transactions. This is an effective and efficient way of communicating within an organization and one of the most effective and useful ways of conducting business [5].

E-commerce can be divided into:

- E-tailing or virtual storefronts on websites with online catalogs, sometimes gathered into a virtual mall
- Buying or Selling on various websites and/or online marketplaces
- The gathering and use of demographic data through Web contacts and social media
- Electronic Data Interchange (EDI), the business-to-business exchange of data
- E-mail and fax and their use as media for reaching prospective and established customers
- Business-to-Business buying and selling
- The security of business transaction [5].

The companies dealing in E-commerce need to maintain huge amount of customer related data and also need to protect these data from various security threats. There are various security standards to address these security issues. This paper will propose a model of implementation of PCI DSS using ISO27001, with reduced complexity, in order to minimize resources, efforts and cost of achieving compliance [2].

2 Mapping ISO 27001 and PCI DSS requirements:

2.1 PCI Data Security Standard:

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) Below is a high-level overview of the 12 PCI DSS requirements [3].

Build and Maintain a Secure Network	1 Install and maintain firewall configuration to protect cardholder data
	2 Do not use vendor-supplied default for system passwords and other security parameter
Protect Cardholder data	3 Protect stored cardholder data
	4 Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability Management Program	5 Use and regularly update anti-virus software or programs
	6 Develop and maintain secure system and applications
Implement Strong Access Control Measures	7 Restrict access to cardholder data by business need to know
	8 Assign a unique ID to each person with computer access
	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 system and processes
Maintain and Information Security Policy	12 Maintain a policy that addresses information security for all person [3].

2.2 Why PCI DSS?

Because the rate of credit card fraud and identity theft is rapidly increasing every year, millions of customers and businesses are affected every day Demonstrating compliance with PCI DSS helps to maintain good business relationships between the service providers, merchants, and acquiring banks The development of the PCI DSS is important to the Payment Card Industry because it minimizes the chances of compromise, it can be used as a measuring stick that gauges data security at the merchant level (GFI), limit risk, may increase revenue, protect consumer data, and help to gain consumer confidence in the industry [3].

2.3 ISO 27001 Standard:

ISO 27001 is an internationally recognized and independent specification for information security management It provides an extensive checklist of best-practice security controls which must be considered for use in the organization's information security control framework These controls include technical, procedural, HR and legal compliance controls and a rigorous system of internal and independent external audits[4].

The ISO 27001 Standard presents a code of practice for information security management, enumerating 133 security controls stated in ISO27002, grouped into 11 groups:

- Security policy
- Organizing information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance [3].

The Standard has been widely perceived as a benchmark for excellence in information security and a process framework for information security governance The ISO 27001 standard is applicable to a very wide range of information systems, identifying security controls in a generic (technology independent) manner and defining a risk-based process for the systematic selection of security controls which are based on the outcome of risk assessment and risk management processes Probably the most important point in the implementation of ISO 27001 the definition of scope which represents part of the business which is actually the subject of certification. A company can certificate processes, systems or organization, depending on its needs. The implementation of ISO 27001 implies two excellent things: management

commitment and security awareness training and continuous improvement plans.The result of the implementation of ISO 27001 should be well established information security management system for a predefine scope, which streams towards continuous improvement Certification of ISO 27001 is a continuous process. Once you are compliant with Standard's controls and external auditor confirms it, certificate must be renewed on a yearly basis Both standards contribute to information security maturity level and for a company which has kind of e-commerce service in its service portfolio, it is recommended to obtain both ISO 27001 and PCI DSS standards [4].

3 Matrix for Mapping of ISO 27001 and PCI DSS requirements

PCI DSS (Requirement)	ISO 27001 (Controls)
1. Install and maintain a firewall configuration to protect data	**A7.** Asset Management
	A10.6. Network Security Management
	A11.4. Network Access Control
2. Do not use vendor-supplied default for system password and other security password	**A10.**Communication and operation management
	A11. Access Control
	A12. Information systems acquisition, development and maintenance
3. Protect stored data	**A10.** Communication and operation management
	A12. Information system acquisition, development and maintenance
	A15. Compliance
4. Encrypt transmission of cardholder data sensitive information across public networks	**A10.** Communication and Operation management
	A11. Access Control
5. Use and regularly update antivirus software	**A10.4**. Protection against malicious and mobile code
6. Develop and maintain secure systems and applications	**A10.** Communication and operation management
	A11. Access Control
	A12. Information systems acquisition, development and maintenance
7. Restrict access to data by business need to know	**A8.1.1.** Roles and responsibilities
	A8.3.3. Removal of access right
	A11. Access Control
8. Assign a unique ID to each person with computer access	**A8.** Human Resource security
	A10. Communication and operation management
	A11. Access Control
9. Restrict physical access to cardholder data	**A8.**Human Resource security
	A9. Physical and Environment security
	A10. Communication and operation management
10. Track and monitoring all access to network resource and cardholder data	**A10.** Communication and operation management
	A11. Access Control
11. Regularly test security systems and information security systems with all control specified in accordance with system and processes	**A10.** Communication and operation management
	A11. Access Control
	A12. Information systems acquisition, development and maintenance
12.Maintain a policy that address information security	**A5.**Security Policy
	A6.Organization of Information security
	A10. Communication and operation management
	A12. Information systems acquisition, development and maintenance [4].

4 Conclusion:

From the above matrix we can draw the following conclusion-

1. The most applicable requirements of ISO27001 to PCI DSS are those which are concern about Communications and operations management, Access control and Information systems acquisition, development and its maintenance.
2. ISO 27001 should be used as a base for all others security standards, even if not officially compliant i.e. without obtained certificate.

3 Standard with such a specific design like PCI DSS should be used in conjunction with a security standard such as ISO/IEC 27001 to successfully achieve a strong Information Security Management System (ISMS) that gives more understand to what controls are in place and being managed.

4. Implementing the management systems aspect of ISO/IEC 27001, which also ensures continuous improvement of an organization's information security program by embracing the proven Plan-Do-Check-Act continuous improvement cycle.

References

1. PricewaterhouseCoopers LLP, **"Revolution or evolution Information Security 2020",** Technology Strategy Board, 2010, **http://www.pwc.com.au/consulting/assets/risk-controls/Revolution-or-Evolution-2010.pdf**
2. Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 1.2.1, July 2009, **https://www.securitymetrics.com/docs/pci_dss_v1-2.pdf**
3. B. Monika, **Compliance Standards in Data Security Why PCI DSS and ISO/IEC 27001 Should Be Integrated**, Georgia Institute of Technology College of Computing & eFortresses Inc., April 30 2010, **http://www.efortresses.com/eFortresses-ISO27001-PCI-Integration-Paper.pdf**
4. L. Zrinka, **Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard**, Central European Conference on Information and Intelligent Systems, P 347-351, September 2012, **http://www.ceciis.foi.hr/app/public/conferences/1/papers2012/iss8.pdf**
5. E- commerce, http://en.wikipedia.org/wiki/E-commerce , date accessed Jan 15 2014

