Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard

Zrinka Lovrić
Hrvatski Telekom d.d.
Savska 32, Zagreb
zrinka.lovric@t.ht.hr

Abstract. *Information security has become very important part of everyday business of most companies. The company's need to protect its valuable assets, material or non material, results in establishing information security management systems and in obtaining various security certificates. To become compliant with internationally recognized certificate, a lot of work needs to be done and a lot of resources must be spent. Major and probably the most common security certificate is ISO 27001. All merchants and service providers of e-commerce and card payment service have to be compliant with PCI DSS. A model of how to reduce required resources and how to simplify achieving PCI DSS compliance by using ISO 27001 will be shown in this paper.*

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

1 Introduction

Since you were little kid, you have been learned how to recognize the potential risk in your environment and how to minimize it or to avoid it. Now the playground is transferred into a corporation where you do the same, on a daily basis, for a common good, even if you are not aware of it.

Very often you read about different data thefts, security breaches, frauds and similar, happened to big companies like Sony, Deutsche Telekom etc. Without strongly developed security awareness level of every employee, together with management support in security questions, nothing else but information security disaster could be expected.

There is a strong need of every company to protect its valuable assets – material like network infrastructure, e.g. or non material, like customer data. Usually companies establish their own, personalized information security management systems, supported by various security mechanisms and strengthen with different security certificates which confirm that the existing security level meets requirements of internationally recognized security standards.

Obtained certificate implicitly alludes on proactivity in handling security risks in order to avoid potential damage and ensures certain confidence in customers' eyes.

2 The Aim

In order to establish secure information systems and in the same time achieve a security benchmark, companies become compliant with different security standards. Compliance with a standard is confirmed by obtaining a certificate. Usually companies have more than one security certificate, due to specificity of their business needs. To become compliant with any standard, depending on a maturity level of company's information security, certain amount of time and other resources is needed. Often it represents a very complex work and a big cost for a company.

Probably the most common security standard is ISO/IEC 27001, the Information Security Management System. It is designed to apply to a wide variety of organizations across numerous industries [11]. ISO controls are suggested controls, and each organization has the flexibility to decide which controls it wants to implement and the compliance is voluntary [4].

ISO 27001 controls do not prescribe in detail how to protect your valuable asset, but compliance with the Standard is a very good basis in achieving a satisfactory level of maturity of information security.

To build up the maturity level, companies obtain other security certificates too. One of them, prescribed by Payment Card Industry Data Security Standard Council, and mandatory for all

merchants and service providers who offer e-commerce and card payment as their service, is PCI DSS Standard.

PCI DSS (Payment Card Industry Data Security Standard) is a widely 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 [11]. It 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.

At first sight, these two standards do not have much in common. If company wants to have both standards, resources and a complexity of their certification double.

Some previous works dealt with comparison of these two standards, mapping the requirements, in more or less detailed manner [2] [11] [12]. The focus was on mapping the matches between standards, without proposing a solution how to simplify implementation of both standards and do some savings.

This paper will propose a model of implementation of both standards, with reduced complexity, in order to minimize resources, efforts and costs of achieving compliance.

3 Mapping ISO 27001 and PCI DSS requirements

3.1. ISO 27001 Standard

The ISO 27001 Standard presents a code of practice for information security management, enumerating 133 security controls stated in ISO 27002, grouped into 11 groups:
1. Security policy
2. Organizing information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance [9]

The Standard has been widely perceived as a benchmark for excellence in information security and a process framework for information security governance [2]. 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 [11]. 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 predefined 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.

3.2. PCI DSS

PCI DSS [1] provides a baseline of technical and operational requirements designed to protect cardholder data.

PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. It consists of over 200 controls grouped into 12 requirements:
1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor–supplied defaults for system passwords and other security passwords.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and information security management systems with all controls specified in accordance with systems and processes
12. Maintain a policy that addresses information security.

It is relatively new security standard, in its form exists since 2006. Compliance validation requirements are different for merchants and service providers and they vary depending on the size of the company and its transaction /business throughout.

PCI DSS does not have formally defined scope, but it is always the same: requirements apply to all system components, defined as any network component, server or application included in, or connected to the cardholder data environment.

The Standard's requirements or controls are mandatory - if an organization wants to comply with PCI DSS then it must comply with every requirement laid out in the Standard. The controls are much very specific and their granularity should, in theory, make auditing of PCI DSS easier [11].

The result of compliance with PCI DSS standard should be developed system of adequate protection of very sensitive cardholder data.

Compliance with PCI DSS standard in order to get a certificate can be achieved by an audit made by external certified assessor, but in combination with quarterly network scanning. If service provider is the entity in process of achieving compliance and if it has less than 300 000 transactions per year per card type, there is no need for external audit, the fulfilled self assessment questionnaire is enough to confirm compliance [1].

3.3. Overlapping of ISO 27001 and PCI DSS requirements

In previous two paragraphs main differences between ISO 27001 and PCI DSS are stated. Although the differences are significant, these two standards overlap in many segments. Probably the most important reason why companies obtain all security certificates, these two comprised, is the potential damage if there are no security controls established and ensured by some worldwide known security standard:

- Financial penalties
- Negative publicity
- Loss of consumer and supplier confidence
- Reduction in revenue [2]

.

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.

ISO 27001 can be perceived as a general security standard and PCI as a specific one. In accordance with common sense, ISO 27001 is the first one to be acquired. Once there are basis, there must be at least a part of it to be used for PCI DSS certification. In Table 1 the overlapping of security requirements of both standards is shown:

Table 1 – overlapping of PCI DSS and ISO requirements

PCI DSS [1]	ISO 27001 [10]
1. Install and maintain a firewall configuration to protect data.	**A10**.6. Network Security Management
	A11.4. Network Access Control
2. Do not use vendor–supplied defaults for system passwords and other security passwords	**A10**. Communications and operations management
	A11. Access Control
	A12. Information systems acquisition, development and maintenance
3. Protect stored data	**A10**. Communications and operations management
	A12. Information systems acquisition, development and maintenance
	A15. Compliance
4. Encrypt transmission of cardholder data and sensitive information across public networks.	**A10**. Communications and operations management
	A11. Access Control
5. Use and regularly update anti-virus software	**A10**.4. Protection against malicious and mobile code
6. Develop and maintain secure systems and applications.	**A10**. Communications and operations 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 rights
	A11. Access Control
8. Assign a unique ID to each person with computer access.	A8. Human Resources security
	A10. Communications and operations management
	A11. Access Control
9. Restrict physical access to cardholder data.	A8. Human Resources security
	A9. Physical and Environmental Security
	A10. Communications and operations management
10. Track and monitor all access to network resources and cardholder data.	**A10**. Communications and operations management
	A11. Access Control
11. Regularly test security systems and information security management systems with all controls specified in accordance with systems and processes.	**A10**. Communications and operations management
	A12. Information systems acquisition, development and maintenance
12. Maintain a policy that addresses information security.	All [12]

Since there are over 200 controls in PCI DSS and each of them can be at least partially mapped with ISO 27001 controls, this is just a high level overview, made by requirement, not by controls.

From the Table 1 it can be concluded that the most applicable requirements of ISO27001 to PCI DSS are those concerning Communications and operations management, Access control and Information systems acquisition, development and maintenance.

5 Conclusion

Implementation of ISO 27001 and PCI DSS standards can be simplified with significant reduction of needed resources, if considered the following model:

- Implement ISO 27001 first, with special stress on Access control and physical security
- Generalize as much as possible the application of ISO 27001 controls, especially of the supporting documentation so it can be applicable even out of predefined scope
- Make ISO 27001 controls obligatory in order to establish the most organized information security management system possible
- Start with PCI DSS implementation when you have already reached certain security maturity level
- Map ISO 27001 and PCI DSS controls, use all you can from already implemented ISO 27001 standard
- Use ISO 27002 control *A8.2.2. Information Security Awareness, Education and Training* as a best practice for raising security awareness level of employees because the maturity level depends partly on their acts
- Include PCI DSS compliance in your security requirements for application and network development so that you are continuously compliant, no matter how new the application is, if it is developed from scratch in accordance with the standard.

The stated model is a result of conducting both ISO 27001 (re)certification and PCI DSS certification, combined with mapped

requirements, available best practices and scientific papers.

ISO 27001 should be used as a basis for all others security standards, although if not officially compliant i.e. without obtained certificate.

6 Future work

In Croatia no company is regulatory obliged to be compliant with ISO 27001 or with PCI DSS standards. But, Croatian National Bank [13] prescribes mandatory information security requirements for all credit institutions. Those requirements are actually ISO27001 requirements adapted to Croatian credit institutions' needs so in fact, all credit institutions are more or less ISO27001 compliant, although most of them do not own the certificate. If they are not compliant, they break the law and they should be subjected to law suits.

The Payment Card Industry Security Standards Council obliges all merchants/service providers of e-commerce and card payment service to be compliant with PCI DSS standard. In case of a security breach, data theft or fraud, merchant/service provider that does not own PCI DSS certificate gets the penalties up to 500 000 $ [1].

I believe that there is no company that has only ISO 27001 and PCI DSS for dealing with security. Most of them have also implemented ITIL and/or CoBIT, and/or SOX controls and many other different security supporting frameworks, best practices, controls etc. Implementation of each of it costs and there is certain overlapping between them.

In my future work I intend to examine a little bit more detailed the status of obtained security certificates and implemented frameworks and controls in Croatia, to compare the existing trends in security here, in a small country on the door of the European Union and the existing trends in the EU. When the trends will be identified, the model of implementation of different security standards and frameworks and controls will be proposed, with highlighted spots where the implementation can be simplified and cost reduced.

References

[1] **PCI DSS v.2**, PCI DSS Council, 2011, available on: www.pcisecuritystandards.org

[2] Rolingson, R., Winsborrow, R.: **A comparison of the Payment Card Industry Data Security Standard with ISO17799**, Computer Fraud&Security, p.16-19, UK, 2006

[3] Ataya, Georges: **PCI DSS Audit and Compliance**, Information security technical report 15, p.138-144, UK, 2010

[4] Rees, James: **The challenges of PCI DSS compliance,** Computer Fraud&Security, p.14-16, UK, 2010

[5] Morse, E.A., Raval, V.: **PCI DSS: Payment Card Industry Data Security Standard in context,** Computer Law&Security Report, p.540-554, UK, 2008

[6] Everett, Cath: **Is ISO 27001 worth it?** Computer Fraud&Security, p.5-7, UK, 2011

[7] Broderick, J.Stuart: **ISMS, security standards and security regulations,** Information security technical report 11, p.26-31, UK, 2006

[8] Pardo, C., Pino, J.F., Garcia, F., Piattini, M., Baldasarre, M.T.: **An ontology for the harmonization of multiple standards and models**, Computer Standards & Interfaces 34, p.48-59, UK, 2012

[9] **HRN ISO/IEC 27001:2006**, HZN Glasilo, 03/2006, Zagreb, Croatia, 2006

[10] **HRN ISO/IEC 27002:2006**, HZN Glasilo, 03/2006, Zagreb, Croatia, 2006

[11] Wright, Steve: **Using ISO 27001 for PCI DSSCompliance,** available at: http://www.insight.co.uk/files/whitepapers/Using%20ISO%2027001%20for%20PCI%20DSS%20Compliance%20(White%20paper).pdf, Accessed: 24th April 2012

[12] Kamat, Mohan: **Mapping ISO 27001 Controls to PCI-DSS V1.2 Requirements, Mapping ISO 27001 Controls to PCI-DSS V1.2 Requirements** available at: http://www.iso27001security.com/ISO27k_Mapping_ISO_27001_to_PCI-DSS_V1.2.pdf, Accessed: 24th April 2012

[13] **Zakon o kreditnim institucijama**, available at: http://www.zakon.hr/z/195/Zakon-o-kreditnim-institucijama, Accessed: 27th April 2012