Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard

Davor Maček,
Zagrebačka Banka d.d.
Samoborska 145, 10000 Zagreb, Croatia
davor.macek@gmail.com

Ivan Magdalenić, Nikola Ivković
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42 000 Varaždin, Croatia
{ivan.magdalenic, nikola.ivkovic}@foi.hr

Abstract. *This paper describes methodology of finding potential risks of bank's noncompliance with Payment Card Industry Data Security Standard (PCI DSS) v2.0 mandatory security requirements. For different types of information assets or security requirements it is necessary to apply different methods of security risk assessment or different standards for specific environment. In this paper, PCI DSS security requirements are explained, Analytic Hierarchy Process (AHP) technique is used as a groundwork to decide which PCI requirements are the most critical and the OCTAVE method is used for formal risk assessment of the most significant PCI requirement in case the requirement is not satisfied. Both, AHP technique and OCTAVE method are applied to a real case scenario in the bank before conducting PCI auditing process.*

Keywords. Risk assessment, information security, PCI DSS, compliance, AHP, OCTAVE, financial institution, bank

1 Introduction

In today's globally networked and complex business environment using some kind of debit or credit or any other kind of cards has become widely accepted. In many stores, hotels and e-commerce transactions using cards is even mandatory because of personnel identification and security.

According to management consultant guru Peter Drucker which famously once said "If you can't measure it, you can't manage it" [4], it is already well known that the first step in the protection of any kind of information in every organization must be security risk assessment of equipment and procedures used for information gathering, processing, storage and distribution. This is very important for financial institutions, particularly those dealing with payment card business, because the exploitation of vulnerabilities in information security for payment cards and supporting infrastructure can lead to significant financial losses and also can have many other negative implications. So, payment card information transmitted or stored in PCI environment of any financial institution must always be suitably protected.

This paper presents mandatory PCI DSS security requirements for cardholder organizations, Analytic Hierarchy Process (AHP) technique for multiple criteria decision making and OCTAVE method for risk assessment.

The paper is organized as follows: Related work is presented along with PCI DSS security requirements in section 2. AHP research methodology and the AHP model for determining of the critical PCI requirement are presented in sections 3 and 4. That is followed by section 5 with security risk assessment of the critical PCI requirement by OCTAVE method. The conclusion is given in section 6.

2 The Payment Card Industry standards and requirements

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, ATM and POS cards. The PCI DSS are developed and maintained by the founding body called the PCI Council, which comprises organizations like MasterCard Worldwide, Visa International, American Express, etc.

The Payment Card Industry (PCI) Data Security Standard (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 other entities that store, process or transmit cardholder data [2].

The PCI Standards v2.0 consists of 12 mandatory requirements divided in 6 categories and more than 250 sub-requirements that enable a multi-pronged coverage of information security management. Those PCI requirements may be enhanced by additional controls and practices to further mitigate risks. These requirements are developed around the following key principles (categories):

I. Build and Maintain a Secure Network
   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

II. Protect Cardholder Data
   3. Protect stored cardholder data
   4. Encrypt transmission of cardholder data across open, public networks

III. Incorporate a Vulnerability Management Program
   5. Use and regularly update anti-virus software or programs
   6. Develop and maintain secure systems and applications

IV. Implement Strong Access Control Mechanisms
   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

V. Continuously Monitor and Test Networks for Threats
   10. Track and monitor all access to network resources and cardholder data
   11. Regularly test security systems and processes

VI. Develop and Maintain an Information Security Policy
   12. Maintain a policy that addresses information security for all personnel.

According to PCI Security Standards Council (SSC) announcement, risk assessment along with cloud computing and e-commerce security, is chosen as one of the PCI SSC focus areas for 2012 [3]. Those three groups were elected by some key merchants, financial institutions, service providers and associations, including Barclaycard, SISA Information Security, The UK Cards Association, Trend Micro, etc.

PCI Compliance is a mandatory requirement for organizations that store, process and/or transmit cardholder data. PCI Risk Assessment is a process of identifying threats and vulnerabilities that affect the cardholder environment. PCI DSS requirements 12.1.2. mandates that organizations conduct a formal risk assessment to identify threats and vulnerabilities and document results as per methodologies such as OCTAVE, ISO 27005 and NIST SP 800-30 [1].

For all banks and other financial institutions whose dealing with PCI business in European Union it's mandatory to get through PCI audit at least once per year. Logically, for this reason, PCI risk assessment is required to be done too at least annually before PCI Qualified Security Assessor (QSA) really come to do auditing in particular financial institution.

PCI risk assessment must be done before auditing process, because when qualitative risk assessment is finished then it's quite straightforward to choose adequate protection and prevention measures. These measures for PCI infrastructure must be taken and implemented before conducting PCI audit process.

As per the PCI SSC's Prioritized Approach for PCI DSS Version 2.0, risk assessment now ranks as milestone one. Hence it is one of the most important activities to be conducted early in financial organization's PCI DSS compliance journey, whether organizations are getting compliant for the first time, or undertaking re-certification.

All those mandatory PCI requirements should be carefully discussed, analyzed and implemented in organization's PCI environment. For certain reasons, e.g., lack of time, specific knowledge or experience to implement it all, especially in huge and complex banking systems, some of those PCI requirements should have higher priority than others. In fact, it means that some PCI requirements are indeed critical and must always be implemented first and satisfied. But, those specific and critical requirements cannot be randomly or incidentally chosen, yet must be obtained using adequate methods or technique. For this purpose in our case study the AHP technique was used for multiple criterion decision making. Then, for the same purpose OCTAVE method was used, and finally we made certain result comparisons and conclusions.

3 Research Methodology by using AHP technique

The Analytic Hierarchy Process (AHP) is a structured technique for organizing, analyzing and making complex decisions, which is based on mathematics and psychology.

The AHP is multi-criteria decision-making approach and was introduced by Saaty (1997 and 1994). The AHP is a decision support tool which can be used to solve complex decision problems. It uses a multi-level hierarchical structure of objectives, criteria, subcriteria and alternatives. The pertinent data are derived by using a set of pairwise comparisons. These comparisons are used to obtain the weights of importance of the decision criteria and the relative performance measures of the alternatives in terms of each individual decision criterion [5].

To make a decision in an organized way to generate priorities we need to decompose the decision into the following four steps [6]:

1. Define the problem and determine the kind of knowledge sought.
2. Structure the decision hierarchy from the top with the goal of the decision, then the objectives from a broad perspective, through the intermediate levels (criteria on which subsequent elements depend) to the lowest level (which usually is a set of the alternatives).
3. Construct a set of pairwise comparison matrices. Each element in an upper level is used to compare the elements in the level immediately below with respect to it.
4. Use the priorities obtained from the comparisons to weigh the priorities in the level immediately below. Do this for every element. Then for each element in the level below add its weighed values and obtain its overall or global priority. Continue this process of weighing and adding until the final priorities of the alternatives in the bottom most level are obtained.

4 The AHP model for determining of the critical PCI requirement

The main goal is to find the most critical PCI requirement that must always be implemented first, based on VECTOR matrix criteria.

For criteria selection in AHP technique, in this case, VECTOR matrix was used. VECTOR matrix is free and open source risk assessment method mostly used for defining the priorities of critical risks [9]. Criteria for ranking alternatives in the AHP model are defined depending on appointed problem, i.e. the alternatives and the goal. In this model the goal is to rank the importance of the mandatory PCI requirements and to find the most critical PCI requirement that should always be implemented first in the bank's PCI environment. Since in our model it is essential to find the most critical PCI requirement we use VECTOR matrix method for risk assessment, which we find suitable for this kind of task. In our opinion the VECTOR matrix may very well fit in this AHP model with its nature for security risk assessment and be quite complementary with PCI DSS security requirements.

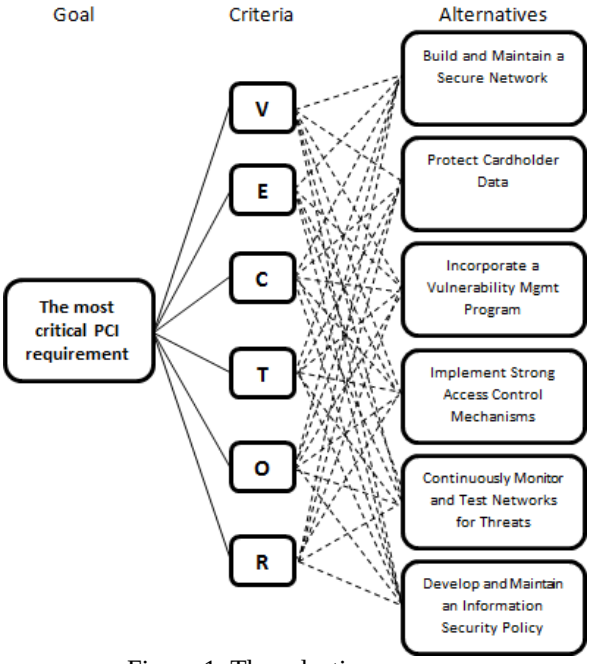

Figure 1. The selection process

VECTOR method for security risk assessment is based on the following formula:

RISK = V+E+C+T+O+R

VECTOR is the acronym derived from the following English words:

V = Vulnerability,
E = Ease of Execution,
C = Consequence,
T = Threat,
O = Operational-Importance,
R = Resiliency.

Hence, the relative importance of VECTOR criteria was made by using judgements in the matrix that is shown in Table 1:

Table 1. VECTOR matrix pairwise comparisons

	V	E	C	T	O	R
V	1	3	0.5	1	3	4
E	0.3333	1	0.3333	2	3	4
C	2	3	1	3	4	5
T	1	0.5	0.3333	1	3	3
O	0.3333	0.3333	0.25	0.3333	1	2
R	0.25	0.25	0.2	0.3333	0.5	1

All the pairwise judgements presented in the Table 1 were made by a small and limited group of information systems security experts responsible for risk assessment.

Using pairwise comparisons, the relative importance of one criterion over another in the matrix can be expressed by this scale:

1 – Equal importance
2 – Weak or slight importance
3 – Moderate importance
4 – Strong importance

5 – Extreme importance

The original scale in AHP technique was 1-9, but for simplicity it was adjusted in this scenario from 1-5 which still fits quite well.

The pairwise comparisons are used to determine the relative importance of each alternative in terms of each criterion. In this approach the decision-makers have to express their opinion about the value of one single pairwise comparison at a time. It can be seen in the VECTOR matrix as there is only one extreme importance in the matrix, which is the relationship between Consequence and Resiliency, and all other pairwise comparisons are mostly slight or moderate. This means that the consequences for the financial institution could be significant in the case of realization of risk.

After setting up pairwise comparisons in the matrix, it is necessary to obtain ranking of criteria. To get a ranking of priorities from pairwise matrix, the eigenvector must be calculated. That is done by squaring the matrix and after that the row sums are calculated and normalized.

The resulting eigenvector weights for VECTOR matrix method are as follows:

Table 2. Eigenvector weights for VECTOR matrix

Vulnerability	0.2289
Ease of Execution	0.1649
Consequence	0.3524
Threat	0.1424
Operational-Importance	0.0658
Resiliency	0.0456

It can be seen from presented eigenvector that the most important VECTOR criterion is **Consequence**.

The next step in AHP model is to determine eigenvectors for alternatives. Computing the eigenvector determines the relative ranking of alternatives under each criterion. In terms of each VECTOR matrix criterion, it is necessary to make pairwise comparisons of mandatory PCI requirements to obtain required eigenvectors. The procedure for calculating eigenvectors of alternatives under each criterion is the same as for determining eigenvector for VECTOR matrix method criteria. This means that in relation to each VECTOR criterion, pairwise comparisons of PCI requirements were done by information systems security experts responsible for risk assessment.

In terms of Vulnerability criterion, where pairwise comparisons determine the preference of each PCI DSS requirement over another, the following matrix is given:

Table 3. Vulnerability criterion – PCI DSS requirements pairwise comparisons

	Secure Network	Protect Cardholder Data	Incorporate Vulnerability Mgmt Program	Strong Access Control Mechanisms	Monitor and Test Networks for Threats	Information Security Policy
Secure Network	1	0.5	1	3	2	4
Protect Cardholder Data	2	1	1	3	3	4
Incorporate Vulnerability Management Program	1	1	1	1	1	1
Strong Access Control Mechanisms	0.3333	0.3333	1	1	2	4
Monitor and Test Networks for Threats	0.5	0.3333	1	0.5	1	3
Information Security Policy	0.25	0.25	1	0.25	0.3333	1

That matrix was squared too and eigenvector was calculated. This procedure was done for every VECTOR criteria in terms of each alternative, namely PCI security requirement. Thus are obtained all eigenvectors according to the criteria of the VECTOR matrix, and those resulting eigenvectors formed a new matrix, as presented in Table 4:

Table 4. Resulting eigenvectors matrix for PCI requirements in terms of each VECTOR criterion

Criteria / Alternatives	V	E	C	T	O	R
Secure Network	0,2290	0,1986	0,1954	0,1142	0,2331	0,2273
Protect Cardholder Data	0,3044	0,1386	0,3327	0,0816	0,3254	0,2631
Incorporate Vulnerability Management Program	0,1504	0,1733	0,1210	0,2057	0,1243	0,1130
Strong Access Control Mechanisms	0,1461	0,2814	0,1954	0,1337	0,1437	0,2137
Monitor and Test Networks for Threats	0,1102	0,1343	0,0853	0,2417	0,1014	0,0995
Information Security Policy	0,0599	0,0738	0,0702	0,2231	0,0721	0,0834

All those calculations were done by Web Java applet called Matrix Multiplier [8].

The final step in this AHP model to get the most critical PCI requirement is to multiply the resulting matrix of eigenvectors from Table 4 with eigenvector weights of VECTOR matrix criteria from Table 2.

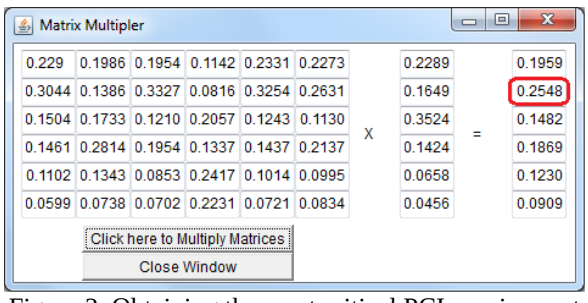

Figure 2. Obtaining the most critical PCI requirement

It can be seen from the Figure 2 above in the rear right-hand column, that is the result of multiplication eigenvector matrices, as the highest value of 0,2548 has the second row which is actually related to the PCI security requirement *Protect Cardholder Data*. Therefore, for the Protect Cardholder Data PCI

security requirement it is necessary to conduct security risk assessment first in the event of its failure by the bank. Security risk assessment of the critical PCI requirement will be conducted by OCTAVE method.

The main reason to do this is that the OCTAVE method can be an excellent addition to the AHP technique. This especially refers to the field of risk assessment criteria that OCTAVE contains in contrast to AHP technique and those criteria form the basis of the OCTAVE method itself. The main risk assessment criteria for the bank in the area of payment card business include bank reputation and client confidence, finance, possible penalties and legal consequences, client's security and productivity. Also, OCTAVE method is much more detailed than AHP technique, which is very important in the final stage of risk assessment process and that would be risk reduction.

A risk assessment report, based on some formal methodology covering the cardholder environment, is required to get PCI DSS v2.0 Compliant.

5 Security Risk Assessment of critical PCI requirement by OCTAVE method

The OCTAVE method is developed at Software Engineering Institute, Carnegie-Mellon University [7]. OCTAVE is a set of tools, techniques and methods for risk assessment and strategic planning of information security. OCTAVE is an acronym of the following English words:

O=Operationally,
C=Critical,
T=Threat,
A=Asset,
VE=Vulnerability Evaluation.

The OCTAVE Allegro, the third and most significant variant of OCTAVE methods will in fact be used for conducting risk assessment of Protect Cardholder Data critical PCI security requirement.

OCTAVE Allegro is a streamlined approach for risk assessing and ensuring information security, designed for large organizations, like banks and other financial institutions.

OCTAVE method is based on the OCTAVE criteria, which are actually standard approach to risk assessment and information security practices. OCTAVE criteria set out the basic principles and attributes of risk management using OCTAVE method. Since financial institutions are generally larger organization, particularly those dealing with business cards, the OCTAVE Allegro method is the most appropriate for them and for conducting risk assessment in case of noncompliance with some PCI security requirements.

In Tables 5-8 is described risk assessment process for Protect Cardholder Data PCI security requirement made by using OCTAVE Allegro method. Also, information security risk assessment is made by the same OCTAVE method for all other groups of mandatory PCI security requirements in case these requirements are not satisfied, but the presentation in this paper is made only for the PCI requirement with the highest score in relation to the AHP model.

Table 5. OCTAVE Allegro – header

OCTAVE Allegro	**RISK ASSESSMENT OF PCI SECURITY REQUIREMENT**
Information asset	Cardholder data
Area of concern	Data of bank's customers can be destroyed, altered or stolen and released because of possible noncompliance with PCI DSS requirement *Protect Cardholder Data* which prescribes that cardholder data must be encrypted in storage and during transmission over open public networks.

Table 6. OCTAVE Allegro – Threat

Actor *Who could exploit the weakness?*	Professional paid hackers or even disgruntled current bank employees
Method *How could the actor exploit the weaknesses?*	Circumventing weak security controls and gaining access to unencrypted data in storage and particularly in transmission by using specially crafted intrusion or sniffing network tools, or even using social engineering techniques.
Motivation *What is the actor's reason for doing it?*	Wants to harm the bank's reputation because of its own status or wants to dispose highly valuable and sensitive data to some interested third party, possible banking competition.
Outcome *What would be the resulting effect on the PCI information asset?*	**Disclosure** **Destruction** **Modification** Interruption
PCI Security requirements *How to violate security requirements?*	Only authorized persons and secure automated banking systems can view, transfer, store or alter cardholder sensitive data.
Probability *What is the likelihood that this threat scenario could occur?*	High **Medium** Low

Table 7. OCTAVE Allegro – Consequences

Consequences *What are the consequences to the financial organization or the information asset owner as a result of the outcome and breach of critical PCI security requirement?*	**(8) Severity of consequences** *How severe are these consequences to the financial organization or asset owner by impact area?*		
	Impact area	**Value**	**Score**

In the case of disclosure clients' account information, the bank is exposed to high reputational risk with the possible loss of confidence and clients.	**Bank reputation and client confidence**	**High**	12
	Finance	**High**	10
Significant labor charges will be required to audit and repair destroyed or modified data.	**Productivity**	Med	7
	Clients' security	Med	8
Exposure of customers' data may lead to fines and possible lawsuits.	**Penalties and legal consequences**	High	10
The relative risk score			**47**

Table 8. OCTAVE Allegro – Risk reduction

Risk Reduction *What action will be taken based on the total score for this risk?*	*Acceptance* *Delaying* ***Reduction*** *Transfer*
For the risk to be reduced, it is necessary to do the following:	
On what container should be applied PCI security requirements and controls?	*What administrative, technical and physical controls will be applied to the container? What residual (remaining) risk would still be accepted by financial organization?*
Cardholder data storage and databases	• Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes • Do not store sensitive authentication data after authorization, even if those are encrypted • Mask Primary Account Number (PAN) when displayed • Make PAN unreadable anywhere it is stored • Protect any keys used to secure cardholder data against disclosure and misuse • Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data • The remaining risk for the bank is that employees and other parties with a legitimate business need can see full PAN of the client
Cardholder data networks	• Use strong cryptography and security protocols (e.g., SSL/TLS, IPsec, SSH) to safeguard sensitive cardholder data during transmission over open, public networks and over local intranet

The reason why the criterion bank reputation and client confidence has a maximum value of risk (12) lies in the fact that in the event of failure of the critical PCI requirement Protect Cardholder Data, the bank may be denied the PCI certification, which may lead the bank to lose the opportunity of dealing with payment card business. This could cause major negative consequences, both for the bank itself and the business and social environment in which the bank works and acts.

It can be seen from Table 7 that the relative risk score is 47, which was obtained by the sum of all values in the impact area. All of these individual values were obtained by expert consultations for information security in the domain of PCI environment. As mentioned earlier, risk assessments were made for other groups of mandatory PCI security requirements and the results are matching.

6 Conclusion

In our opinion a PCI risk assessment has a potential to bring tremendous value to the PCI community. For financial organizations dealing with PCI business, a PCI risk assessment should be a starting step before they go into a full transition to PCI QSA (Qualified Security Assessor) audit.

It can be concluded that the potential threats that are able to exploit existing vulnerabilities of the banking system can cause major negative effects on the PCI security requirement called Protect Cardholder Data, and can have severe consequences if bank is noncompliant with it. The final results of our methods stress the importance of protecting banking information systems and especially sensitive user data. Calculation results show the fundament what actually needs to be protected in the banking information systems and first of all that would be sensitive user data.

Also, it can be concluded that the AHP technique is more formal and precise than the OCTAVE method, because the AHP has resulted from mathematical model, but not as expressive as the OCTAVE method itself. It can be said that AHP technique, because of its proven mathematical model, serves as a great groundwork to OCTAVE method for information security risk assessment. But the OCTAVE method is still necessary to supplement with certain solid mathematical model of the criteria for assessing risk and defining their values.

Considering that there still exists some part of the subjective risk assessments of computer professionals for information security in relation to certain areas of influence on the PCI environment, future research will focus on how to get firmer mathematical

foundation for these results. This would reduce the possibility of human error in the information security risk assessment for particular area.

References

[1] SMART: The World's First PCI Risk Assessment Tool, PCI Risk Assessment, available at http://smart-ra.com/pciriskassessment.aspx, Accessed: 15th March 2012.

[2] PCI Security Standards Council: Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0, October 2010.

[3] PCI Security Standards Council (SCC): Press Release, available at https://www.pcisecuritystandards.org/pdfs/pr_111511_2012_SIG_Projects_Press_Release_FINAL.pdf, Accessed: 15th March 2012.

[4] Risk Watch International: Risk Watch Solutions for Risk Assessment of Information Systems, available at http://riskwatch.com/index.php/information-systems, Accessed: 15th March 2012.

[5] E. Triantaphyllou, S. H. Mann: Using the analytic hierarchy process for decision making in engineering applications: some challenges, Inter'l Journal of Industrial Engineering: Applications and Practice, Vol. 2, No. 1, pp.35-44, 1995.

[6] T. L. Saaty: Decision making with the analytic hierarchy process, Int. J. Services Sciences, Vol. 1, No. 1, pp.83–98, 2008.

[7] R. A. Caralli, J. F. Stevens, L. R. Young, W. R. Wilson: The OCTAVE Allegro Guidebook, v1.0, Software Engineering Institute, Carnegie Mellon, May 2007, available at http://www.cert.org/octave/allegro.html, Accessed: 29th October 2010.

[8] JoeMath.Com Official Web Site of Joe McDonald: Matrix Multiplying Calculator, available at http://www.joemath.com/applets/multmat/, Accessed: 20th March 2012.

[9] VECTORMatrix.com – Risk Assessment Methodology, Security, Impact Articles, U.S. Ravias Corp, available at http://www.riskvector.com, Accessed: 15th April 2012.