Appendix B

Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Version: 2.0

Date: November 2012

Author: Risk Assessment Special Interest Group (SIG)
PCI Security Standards Council

Information Supplement:

PCI DSS Risk Assessment Guidelines

Table of Contents

1 Introduction

1.1 Objective

The objective of this document is to provide supplemental guidance and recommendations for performing a risk assessment in accordance with PCI DSS Requirement 12.1.2.

A risk assessment, as required in the PCI DSS, is a formal process used by organizations to identify threats and vulnerabilities that could negatively impact the security of cardholder data.

This document does not replace, supersede, or extend any PCI DSS requirements; rather it provides guidance for organizations to identify, analyze, and document the risks that may affect their cardholder data environment (CDE).

1.2 Intended Audience

This guidance is intended for any organization that stores, processes, or transmits cardholder data (CHD). Examples include merchants, service providers, acquirers (merchant banks), and issuers. The intended audience includes large, medium, or small organizations.

2 Risk Assessments and the PCI DSS

2.1 Risk Definition

Risk has many interpretations, and is often used to describe dangers or threats to a particular person, environment, or business. The following is just one definition:

> *Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization*[1]

Understanding risk includes understanding of the different elements and how they fit together. For example, considerations from a business perspective may include:

- What are the different types of threats to the organization?
- What are the organization's assets that need protecting from the threats?
- How vulnerable is the organization to different threats?
- What is the likelihood that a threat will be realized?
- What would be the impact if a threat was realized?
- How can the organization reduce the likelihood of a threat being realized, or reduce the impact if it does occur?

2.2 PCI DSS Requirement 12.1.2

PCI DSS Requirements	Testing Procedures
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).
12.1.1 Addresses all PCI DSS requirements.	**12.1.1** Verify that the policy addresses all PCI DSS requirements.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	**12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.
	12.1.2.b Review risk assessment documentation to verify that the risk assessment process is performed at least annually.

Figure 1.0 – PCI DSS Requirement 12.1.2

PCI DSS Requirement 12.1.2 requires organizations to establish an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.

[1] NIST SP800-30

A risk assessment enables an organization to identify threats and the associated vulnerabilities which have the potential to negatively impact their business. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threats being realized.

Performing risk assessments at least annually allows organizations to keep up to date with business changes and provides a mechanism to evaluate those changes against the evolving threat landscape, emerging trends, and new technologies. Examples of changes include the introduction of a new product line or service offering that is different from existing products or services, introduction of a new software application in the CDE, change of a network topology impacting the CDE, etc.

2.3 Risk Management Strategy

Because the PCI DSS risk assessment takes into account only a subset of the organization's overall risks, organizations should maximize the benefits of a risk assessment by incorporating the PCI DSS risk assessment into their overall organization-wide risk management program.

The risk assessment process should include people, processes, and technologies that are involved in the storage, processing, or transmission of CHD including those that may not be directly involved in processing CHD but still have the potential to impact the security of the CDE—for example, perimeter building security at the facility where the CDE is located. Consideration should also be given to business processes outsourced and/or managed by third-party service providers or merchants.

To ensure adequate coverage, an organization-wide risk management program would need to ensure that risks across all areas of the organization are considered, that there is a coordinated strategy for addressing identified risks, and that the risk mitigation efforts are aligned across all business processes.

2.4 PCI DSS Requirements

PCI DSS provides a baseline of technical and operational controls that work together to provide a defense-in-depth approach to the protection of cardholder data. PCI DSS comprises of a minimum set of requirements for protecting cardholder data and may be enhanced by additional controls and practices to further mitigate risks. Risk assessments provide valuable information to help organizations determine whether additional controls are necessary to protect their sensitive data and other assets.

Note: *The result of a risk assessment must not be used by organizations as a means of avoiding or bypassing applicable PCI DSS requirements (or related compensating controls).*

In order to achieve compliance with the PCI DSS, an organization must meet all applicable PCI DSS requirements.

2.5 Benefits of Conducting a PCI DSS Risk Assessment

Conducting a PCI DSS risk assessment helps an organization to identify and understand the potential risks to their CDE. By understanding these risks, an organization can prioritize risk-mitigation efforts to address the most critical risks first. Organizations can also implement threat-reducing controls more effectively, for example, by choosing a technology or solution that best addresses identified risks.

Risk assessments can help identify the presence of cardholder data that is not fundamental to business operations and that can be removed from an organization's environment, reducing both the risk to the environment and potentially the scope of their CDE.

In addition, risk assessments can identify areas containing data that need protection versus areas that are more open and do not need access to sensitive data. Information obtained through a risk assessment can be used to determine how to segment environments to isolate sensitive networks (CDE) from non-sensitive networks and, thus, save unnecessary investment in security controls where they are not needed. Isolation of these less sensitive networks helps to define the CDE and contributes to an effective scoping methodology.

Performing risk assessments at regular intervals provides an organization with the insight into changing environments and assists it to identify where mitigation controls need to be adjusted or added before new threats can be realized. This practice may provide the opportunity to identify whether future investment in resources may be warranted.

Ideally, a continuous risk assessment process would be implemented to enable ongoing discovery of emerging threats and vulnerabilities that could negatively impact the cardholder data environment (CDE), allowing an organization to mitigate such threats and vulnerabilities in a proactive and timely manner.

2.6 Risk Assessment and the Prioritized Approach

For organizations working towards their initial PCI DSS compliance validation, the PCI DSS Prioritized Approach provides a roadmap of compliance activities based on risks associated with storing, processing, and/or transmitting cardholder data. It helps organizations prioritize efforts to achieve compliance, establish milestones, and lower the risk of CHD breaches early in the compliance process. As part of Milestone 1, the organization needs to implement a formalized risk assessment process to identify threats and vulnerabilities that could negatively impact the security of their cardholder data.

Organizations working towards compliance may find that the initial risk assessment requires additional time and resources, as it may be the first time the environment has been reviewed and evaluated from a risk-based perspective. Furthermore, if a risk assessment process is not already established, organizations will need to define and document their risk assessment methodology, identify individuals who will need to be involved, assign roles and responsibilities, and allocate resources.

For organizations maintaining compliance, it is important to understand that the annual PCI DSS validation is only a snapshot of compliance at a given time, as noted on the Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). To ensure compliance is maintained, a risk assessment may be undertaken after any significant changes to the CDE including, but not limited to, any changes in technologies, business processes, personnel, and/or third-party relationships that could impact the security of CHD.

3 Industry-Standard Risk Methodologies

3.1 Common Elements

A number of industry-accepted methodologies are available to assist organizations to develop their risk assessment process. Examples of these methodologies include:

- **International Organization of Standardization (ISO)** has published a wide array of standards appropriate to information security and risk management. The most relevant document for understanding and providing guidance on risk assessment is *ISO 27005,* which is a risk management guideline. This document covers the standard information security risk management processes that are undertaken encompassing risk assessment.

  The guidance provided in ISO 27005 is useful for conducting formal information security risk assessments.

- **The National Institute of Standards and Technology (NIST)** develops standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services. Overall guidance on risk management for information systems is covered in Managing Information Security Risk: Organization, Mission and Information System View (NIST SP 800-39), while the NIST SP 800-30 (Revision 1) focuses exclusively on risk assessments. Much of the work conducted by NIST aligns with the work undertaken in Europe by organizations such as ITSEC and subsequently Common Criteria.
- **Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE®)** is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning. The OCTAVE method lists eight processes for a formal risk assessment. It leverages people's knowledge of their organization's security-related practices and processes to capture the current state of security within the organization. Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization. OCTAVE resources provide a useful source for guidance.

Other risk frameworks, such as Factor Analysis of Information Risk (FAIR) and the Australian/New Zealand Standard AS/NZS 4360, can either be used on their own or to supplement assessments performed using traditional methodologies, such as OCTAVE and those published by ISO and NIST.

All of the methodologies mentioned above have common goals, albeit from slightly differing perspectives. They are all suitable for PCI DSS risk assessments. Each risk methodology incorporates the following core activities:

- Identifying critical assets and the threats to those assets
- Identifying the vulnerabilities, both organizational and technological, that could potentially expose assets to those threats, resulting in risk to the organization

- Developing a risk strategy and risk mitigation plans to address identified risks in support the organization's mission and priorities

Many risk assessment methodologies follow similar steps; however the approaches they undertake for identification of risks and their measurement techniques differ. Most methodologies have options for both *quantitative* and *qualitative* approaches (discussed later in this document).

Organizations may choose to incorporate a formalized risk assessment methodology (such as the ones covered above) and adapt it to the culture and requirements of the organization.

4 Key Elements of a Risk Assessment

4.1 Develop a Risk Assessment Team

The risk assessment team should include representation from all the departments within the organization, including those that are involved in the processing, storage, and transmission of CHD. Such departments may include business processes, technology and support departments, such as Human Resources, Marketing, Operations, Information Technology, Information Security and Security Administration.

Where possible it is recommended the risk assessment is led by an individual and/or individuals who have sufficient knowledge of the PCI DSS requirements and the risk assessment methodology being utilized by the organization. The risk assessment process leader is typically responsible for driving the risk assessment process within the organization and reporting the results to management. Organizations without the internal resources or skills to conduct risk assessments may consider engaging external resources to assist with their risk assessment process.

4.2 Building a Risk Assessment Methodology

When developing their own risk assessment methodology, organizations may consider adapting an industry-standard methodology that is most appropriate for their particular culture and business climate, to ensure their particular risk objectives are met. Figure 2.0 illustrates typical risk assessment components.

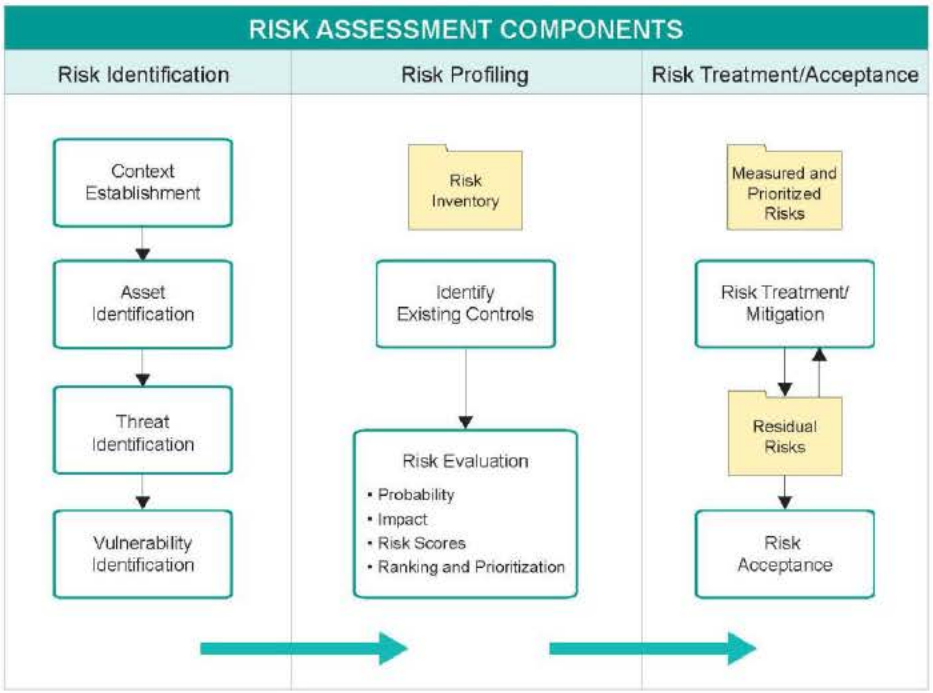

Figure 2.0 – Risk assessment components

4.2.1 Risk Identification

Before an organization can assess its risks, it should understand its business processes, assets, threats, and vulnerabilities.

- **Context Establishment** – The risk assessment team needs to understand the internal and external parameters when defining the scope of the risk assessment and/or have access to the persons in the organization who can provide this information—for example, the organization's hierarchy, business processes, CHD flows, and any associated system components.
- **Asset identification** – Generally, assets could be anything of value to an organization. In the context of PCI DSS, assets include the people, processes, and technologies that are involved in the processing, storage, transmission, and protection of CHD. Each asset may be identified to an asset owner who will then be responsible for adequately protecting the asset. The asset may also be assigned an asset value based on its importance and criticality.

  When identifying assets for a PCI DSS risk assessment, all payment channels should be considered—for example, face-to-face, e-commerce, mail order/telephone order (MOTO), etc.—as the assets identified for each payment-acceptance channel may carry different levels of risk.

  To help categorize the assets as relevant to the organization's business, it may be helpful to structure the assets into groups and sub-groups such as those shown in Figure 3.0:

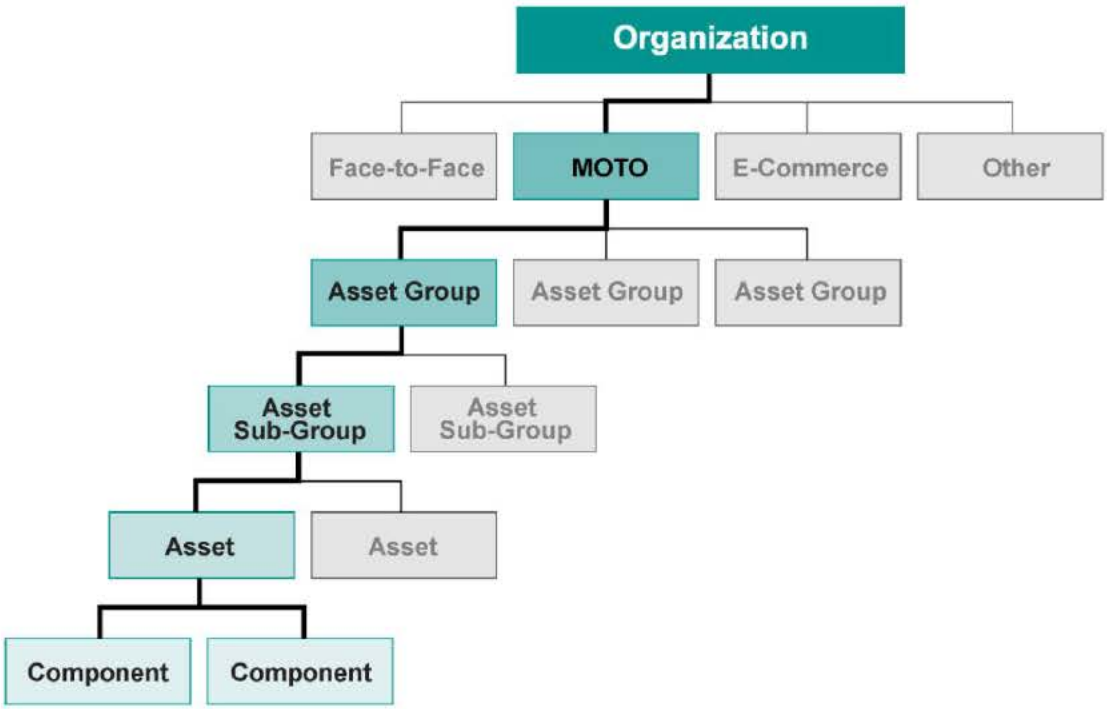

Figure 3.0 - Asset Grouping

- **Threat identification** – Threats may include people, the systems they use, and conditions that could cause harm to an organization. Talking to staff across all areas of an organization will help the risk assessor understand where they see the potential for threats to emerge. Personnel at different levels of the organization will have different perspectives and can provide information that the risk assessor may not have previously considered.

  In addition, security incidents that may have occurred, within either the organization or industry, can be reviewed to help an organization identify potential threats. Threats are commonly measured in terms of the capability of the "threat agent" (anything that has the potential to realize a threat), the intent of the threat agent, relevance to the organization, likelihood that a threat will occur, and the potential for adverse impacts.

- **Vulnerability identification** – A vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organization, the environment, or a business process. In a risk assessment, all vulnerabilities should be considered. For example, vulnerabilities can occur as a result of design, development, and/or deployment deficiencies of systems or software. Organizational and business-process vulnerabilities may exist because of non-existent or ineffective policies and procedures. Vulnerabilities may be identified from vulnerability assessment reports, penetration-test reports and technical security audits such as firewall rule reviews, secure code reviews and database configuration reviews.

Table 1.0 on the following page provides just a few examples of threats and vulnerabilities, together with the possible outcome and impact to an organization's business operations. This is not an exhaustive list, as an organization will encounter many other threats and vulnerabilities that will have the potential to negatively affect their business.

Table 1.0 – Threats, Vulnerabilities, Risk, and Impact

Threats	Vulnerabilities	Potential Outcome/Risk	Potential Impact to Business
External hackers, malicious individuals, cyber criminals	▪ Lack of network security—e.g., properly configured firewalls, lack of intrusion detection ▪ Weak password policy ▪ Transmission of unprotected CHD ▪ Lack of security awareness to social engineering, phishing ▪ Insufficient system hardening, malware protection	▪ Network intrusion ▪ Compromise of user credentials ▪ System compromise ▪ Introduction of malicious code ▪ System downtime ▪ Compromise of sensitive data	▪ Theft of CHD and/or SAD ▪ Reputational impact ▪ Loss of business due to decreased customer confidence ▪ Interruption to business processes ▪ Financial loss—cost of recovery, forensic investigation, lost revenue, possible fines/penalties
Internal malicious individuals, internal user mistakes, human error	▪ Lack of effective change control ▪ Lack of user knowledge/training ▪ Inappropriate assignment of access permissions (e.g., not based on need to know or least privilege) ▪ Lack of separation of duties ▪ Insufficient system hardening ▪ Weak encryption/poor key-management practices	▪ Introduction of malicious code through web browsing/email ▪ Untested system changes ▪ Privilege escalation of user accounts ▪ Unauthorized access to sensitive data	
Thief/intruder intending to cause physical damage or steal assets	▪ Lack of physical security/monitoring ▪ Insecure handling of payment terminals ▪ Lack of tamper-detection ▪ Disposal of storage media without deleting data ▪ Failure to properly supervise visitors/vendors	▪ Theft/replacement of payment terminals ▪ Undetected skimmers added to POS systems ▪ Unintended access to CHD ▪ Installation of rogue devices leading to network compromise	

4.2.2 Risk Profiling

Risk profiling is the presentation of all risks to an asset, together with threats and vulnerabilities and their respective risk scores. Risk profiling enables asset owners to evaluate risks and take necessary risk-mitigation measures.

Risk profiling generally includes the following:

Table 2.0 – Risk Profiling Characteristics

Category	Characteristics
Assets	▪ Asset type (primary or supporting asset, information or business process, hardware or software, etc.) ▪ Asset Value
Threat	▪ Threat Properties (insider or outsider, accidental or deliberate, physical or network, etc.) ▪ Threat likelihood/probability
Vulnerabilities	▪ Vulnerability description ▪ Level of Vulnerability
Risk	Risk score is a function of: ▪ Asset value, ▪ Likelihood of threat, and ▪ Level of vulnerability

4.2.2.1 Existing controls

Existing controls are those that are already present in an organization to protect against the identified threats and vulnerabilities. The identification of existing controls is necessary to determine their adequacy. The effectiveness of existing controls can be identified by reviewing existing policies/procedures, interviewing people, observing processes, and reviewing previous audit reports and incident logs.

4.2.2.2 Risk evaluation

Risk evaluation allows an organization to determine the significance of risks in order to prioritize mitigation efforts. This helps organizations achieve the optimum usage of resources. Risk-measurement techniques used during the evaluation process can be quantitative, qualitative, or a combination of both:

a) **Quantitative risk assessment** – A quantitative risk assessment assigns numerical values to elements of the risk assessment (usually in monetary terms). This is accomplished by incorporating historical data, financial valuation of assets, and industry trends.

Quantitative risk assessments can be regarded as more objective than qualitative risk assessments as they are based on statistical information. However, performing a purely quantitative assessment is often difficult since it may be difficult to determine a monetary value for some assets, such as an organization's "reputation."

b) **Qualitative risk assessment** – Qualitative risk assessments categorize risk parameters according to the level of intensity or impact to an asset. The categorization of risk parameters is accomplished by evaluating the risk components using expert judgment, experience, and situational awareness. The scales are typically based on an escalating set of values—for example, low, moderate, and high.

Tables 2.1 and 2.2 are examples of some commonly used measurement techniques. Table 2.1 evaluates risk as a factor of impact and probability, whereas Table 2.2 represents risk as a factor of asset value, likelihood of threat, and ease of exploitation.

Table 2.1 – Example of a risk calculation matrix

		Consequence		
		Minor Impact	***Moderate Impact***	***Major Impact***
Likelihood	***Very likely***	Medium Risk	High Risk	High Risk
	Likely	Medium Risk	Medium Risk	High Risk
	Possible	Low Risk	Medium Risk	High Risk
	Unlikely	Low Risk	Low Risk	Medium Risk

Table 2.2 – Example of a risk calculation matrix using Asset Value, Threat, and Ease of Exploitation (or Level of Vulnerability)

	Likelihood of Threat	**Low**			**Medium**			**High**		
	Ease of Exploitation	**Low**	**Med**	**High**	**Low**	**Med**	**High**	**Low**	**Med**	**High**
Asset value	***Low***	0	1	2	1	2	3	2	3	4
	Medium	1	2	3	2	3	4	3	4	5
	High	2	3	4	3	4	5	4	5	6
	Very High	3	4	5	4	5	6	5	6	7
	Critical	4	5	6	5	6	7	6	7	8

Low Risk 0-2	Medium Risk 3-5	High Risk 6-8

Qualitative risk assessments are more subjective than quantitative risk assessments but may result in a better understanding of the business, as well as improving communication between the different business departments contributing to the overall risk assessment.

In some cases, numbers are assigned to each value to create a numeric equivalent to the scale. This approach is sometimes referred to as "semi-quantitative" measurement. Such methods are used when it is not possible to use quantitative methods, or when there is a need to reduce the subjectivity in qualitative methods.

Many organizations perform risk assessments using a combination of quantitative and qualitative methods.

4.2.3 Risk Treatment

Once risks have been identified and measured, it is important to define risk treatment strategies. Because the elimination of all risk is usually impractical or close to impossible, it is important to implement the most appropriate controls to decrease risk to an acceptable level. Risk treatment strategies include:

- **Risk reduction** – Taking the mitigation steps necessary to reduce the overall risk to an asset. Often this will include selecting countermeasures that will either reduce the likelihood of occurrence or reduce the severity of loss, or achieve both objectives at the same time. Countermeasures can include technical or operational controls or changes to the physical environment. For example, the risk of computer viruses can be mitigated by acquiring and implementing antivirus software. When evaluating the strength of a control, consideration should be given to whether the controls are preventative or detective. The remaining level of risk after the controls/countermeasures have been applied is often referred to as "residual risk." An organization may choose to undergo a further cycle of risk treatment to address this.
- **Risk sharing/transference**[2] – The organization shares its risk with third parties through insurance and/or service providers. Insurance is a post-event compensatory mechanism used to reduce the burden of loss if the event were to occur. Transference is the shifting of risk from one party to another. For example, when hard-copy documents are moved offsite for storage at a secure-storage vendor location, the responsibility and costs associated with protecting the data transfers to the service provider. The cost of storage may include compensation (insurance) if documents are damaged, lost, or stolen.
- **Risk avoidance** – The practice of eliminating the risk by withdrawing from or not becoming involved in the activity that allows the risk to be realized. For example, an organization decides to discontinue a business process in order to avoid a situation that exposes the organization to risk.
- **Risk acceptance**[2] – An organization decides to accept a particular risk because it falls within its risk-tolerance parameters and therefore agrees to accept the cost when it occurs. Risk acceptance is a viable strategy where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are accepted by default

[2] ***Note:*** *A risk assessment cannot result in the acceptance, transferring, or sharing of any risk that will result in the failure to comply with any applicable PCI DSS requirements.*

5 Third-Party Risks

5.1 Risks Shared With Third Parties

Organizations may outsource business processes, obtain services, or have business relationships with third party merchants, service providers, or other entities that could influence the security of CHD. Performing a risk assessment is essential to understanding the level of risk that could be introduced to the organization by conducting business with third-party merchants and/or service providers. Third parties represent three major areas to consider for risk management: they may introduce risk, they may share risk, or they may manage risk:

	Third Parties may:	Such as:
1	**Introduce risk**	The development of an application that processes, stores, or transmits CHD
2	**Manage risks**	An outsourced business process
3	**Share risk**	A shared business process

Figure 4.0 - Asset Grouping

A single third-party entity can represent all of these areas at the same time and impact the organization's overall risk posture. The first step to understanding the risks posed by third parties is to know the scope of the business relationship or service provided by the third party. To identify every applicable third party, an organization should study their CHD flows and any business processes involving CHD. In addition, an organization should consider third parties that are involved in the development, operation, or maintenance of their CDE (even those who do not directly handle cardholder information could still indirectly have an impact on the organization's CDE). Some examples of third parties and/or service providers to consider include:

- Application developers
- Data-center providers
- Web-hosting providers
- Data-storage providers
- Data/media/hardware-destruction service providers
- Managed services—for example, IT operations, security
- Outsourced operational teams–for example, call centers
- Contractors

It may be helpful to organizations to understand the key attributes of each third-party relationship, including but not limited to whether the third party is PCI DSS compliant (for instances where the CDE is impacted) or whether their payment application is PA-DSS compliant (for application development); the level of the service provider (often based upon transaction volume); whether appropriate legal contracts are in place between the third party and the organization regarding the management of CHD; and the number of people or systems at the third party who have access to the CHD.

Reviewing a third party's key attributes, such as those listed above, will help an organization to establish a risk level for each third party involved in the development, operation, or maintenance of their CDE and help to prioritize those that appear to carry the highest level of risk.

In addition, it should be noted that a third party may itself be dependent upon other third parties for critical PCI-related services. It may not be necessary or appropriate to extend the risk assessment to the second level of third parties but it is appropriate to know that they exist and may have an impact.

5.2 Risk Sharing/Transference

Once a risk assessment is complete, there are a number of risk treatment options that might be possible. These have previously been discussed in Section 4.2.3, Risk Treatment, and each could apply to a third party.

Risk transference is one of the most relevant risk treatment strategies to third parties, and an organization may manage this relationship by written agreement, via a contractual obligation that states that the third party assumes responsibility for the security of CHD they process, store, or transmit on behalf of the organization. However, the remaining reputational risk means it is unlikely that the full risk to an organization will ever be truly transferred.

Written agreements might help put in place processes to mitigate third-party risks, but it is likely that further assurance is needed to assess whether they have the appropriate security controls and processes in place.

Approaches to the management of third-party risks may include a reliance on a PCI DSS assessment of the third party conducted by a QSA and the completion of a ROC, or where the third party attests compliance to PCI DSS via a Self-Assessment Questionnaire. Alternatively, the organization may perform a risk assessment of the third-party merchant and/or service provider with internal resources and/or work with the third party to determine whether the third party is managing an organization's risks to their satisfaction.

It is recommended that the written agreement (as per PCI DSS Requirement 12.8.2) includes the requirement for the third-party merchant and/or service provider to inform the organization if there is an incident that adversely affects an organization's CHD. Additionally, the organization may wish to conduct a risk assessment to determine the impact, steps for remediation, and associated time frames. Regular communication with the third-party merchant and/or service provider is

recommended so that the details of the incident are known and the status can be reported back to the appropriate stakeholders where necessary.

During the risk assessment process, an organization may determine that continuing business with the third-party merchant and/or service provider may increase the organization's overall risk in respect of CHD and may take appropriate measures to reduce their residual risk to an acceptable level. These measures may include the termination of the business relationship with the third party. As part of the annual risk assessment process, any business relationships with third-party merchants and/or service providers should be re-evaluated.

6 Reporting Results

It is suggested that each risk assessment results in a risk assessment report detailing the identified risks, including those affecting the cardholder data environment. The objective of the report would be to clearly articulate the various risks that concern the organization and may also explain the actions taken by the organization to remediate these risks. The following table includes suggested topics that a report may contain.

Table 3.0 – Risk Assessment Reporting Topics

Topic	Explanation of Content
Scope of Risk Assessment	A risk assessment report should clearly describe the organization and the internal and external parameters taken into consideration when defining the scope of the risk assessment. This may include the purpose of the risk assessment, the technologies in place, business processes, third-party relationships, key stakeholders, and any additional pertinent details. For the purpose of PCI DSS Requirement 12.1.2, the scope may also include an overview of the cardholder data environment and the organizations involved in supporting and operating the processing of cardholder data.
Asset Inventory	This process involves making a comprehensive list of assets that are in scope for the risk assessment, for example, software, hardware, networking and communications infrastructure and personnel. An asset inventory may also include asset value, asset type, asset owner, and asset location for each asset identified.
Threats	The threats that can harm the identified assets should be listed. This list may also include a description of each threat to help understand the characteristics of the identified threats. The likelihood of the threats being realized will be calculated based on the risk assessment methodology used by the organization (expressed as either a percentage probability or a qualitative ranking (e.g., low, medium, or high).
Vulnerabilities	The risk assessment report may also contain a list of vulnerabilities, both technological and organization-related, that can affect the organization's assets. The type of threats that are likely to leverage the vulnerability may also be listed.
Risk Evaluation	The report should describe the risk-measurement technique used to prioritize the identified risks—for example, quantitative or qualitative measures.

Topic	Explanation of Content
Risk Treatment	The risk assessment report should document the list of actions taken for each of the risks identified, along with their completion status—for example, risk reduction, risk transference, etc.
Version History	The risk assessment report may include the date, author, and the approver of the document. The risk assessment date can help an organization to monitor the frequency of their risk assessments, and may help to confirm that assessments are performed at least annually as required by PCI DSS Requirement 12.1.2.
Executive Summary	It can be good practice to include an executive summary of the risk assessment report. The executive summary can detail the risk posture of the organization before and after risk mitigation. The summary can also provide a suitable dashboard of risks for management in terms of number of assets, threats, vulnerabilities, and risks.

7 Critical Success Factors

Identification – The correct identification of assets plays an important role in the risk assessment process. Therefore, organizations should gather input from all stakeholders (such as Human Resources, Information Security, business departments, etc.) that are involved in the processing, storage, and transmission of CHD.

To properly identify threats and vulnerabilities, assessors should have an open mind and factor in the various conditions that could negatively impact the CDE. Historical events, audit reports, and security incidents (within the organization or industry) can also provide additional insight.

Proactive approach – The risk assessment process should be proactive instead of reactive. This will allow the organization to proactively identify, analyze, and document their risks. Taking a proactive approach helps organizations avoid costly corrective measures. Therefore, there is a need for the continuous monitoring of risks throughout the year.

Keeping it simple – The risk assessment process can be kept simple by developing a methodology that best suits the needs of an organization. Published industry-standard methodologies may assist in this process.

Measurement scales should be limited to a small number of categories. Inclusion of numerous categories will often introduce unnecessary complexity and reduce the likelihood that risk stakeholders will understand the results. Each value on a measurement scale should be explicitly defined. Without clear definitions, stakeholders will often form differing opinions on the data. Once the measurements are defined, they should be validated by the individuals who participated in the risk assessment process to ensure that the results are interpreted consistently across the organization.

Training – It is also suggested that risk assessors are trained on formal risk assessment processes to ensure they are better prepared to understand the threats and vulnerabilities that could negatively impact the security of cardholder data, and ultimately their organization.

8 Acknowledgements

The PCI SSC would like to acknowledge the contribution of the Risk Assessment Special Interest Group in the preparation of this document. The members include representatives from the following organizations:

ABC Financial Services	Liquid Networx
Accuvant Inc.	Market America, Inc.
Airlines Reporting Corporation	McGladrey LLP
A-lign Security and Compliance Services	Nationwide Building Society
AOL Inc.	PayPal Inc.
Assurant, Inc.	Progressive Casualty Insurance Company
Bank of America N.A.	Protegrity USA, Inc.
Bankalararası Kart Merkezi (BKM) A.Ş.	Retalix
Barclaycard	Royal Bank of Scotland Group
Bell Canada	SecureState LLC
BrightLine CPAs & Associates, Inc.	Security Risk Management Ltd
BT Counterpane	SecurityMetrics, Inc.
Capita Plc	Sense of Security Pty Ltd
CHS INC	SISA Information Security Inc.
CIPHER Security	Sprint Nextel
Citibank NA, Sucursal Uruguay	Store Financial Services, LLC
Coalfire, Inc.	Suncor Energy Inc.
Compass Group UK & Ireland Limited	Symantec Corp.
Crowe Horwath LLP	Tesco
D+H	Thales eSecurity Limited
Deloitte LLP - UK	The Co-operative Group
Deluxe Corporation	The Members Group
First Data Merchant Services	Tripwire, Inc.
Fiscal Systems, Inc.	Trustwave
Global Payments Inc.	TUI Travel PLC
HP Enterprise Security Services	VeriFone, Inc.
IQ Information Quality	Verizon Enterprise Solutions
Kilrush Consultancy Ltd.	Verizon Wireless
LBMC Security Services	Vodat International Ltd
Levi Strauss and Co.	Yum! Brands, Inc.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.