



RISK ADVISORY SERVICES

How can banks and retailers secure PCI DSS compliance?

WN CR & KPMG CR's approach to providing the PCI DSS certifications

Tomáš Kudělka
January 2009

ADVISORY

Contents

Introduction	3
Selection Criteria & Compliance Reports	6
WN CR and KPMG CR's overall approach to the programmes	10
Security Breaches and Vulnerability Experiences	19

The Programme

<p>VISA Account Information Security (AIS) Program</p>	<p><i>The Account Information Security (AIS) Program is a globally mandated program that deals with data security.</i></p> <p>This program accredits merchants, payment processors and service providers against the Payment Card Industry Data Security Standard through a combination of onsite audits and vulnerability assessments. The program is run on a regional basis by VISA's regional organisations. Both VISA Europe and VISA US are fully aligned with the program with other regions following the same standards with different selection criteria (see later).</p>
<p>MasterCard Site Data Protection (SDP) Program</p>	<p><i>The MasterCard Site Data Protection program (SDP) provides a comprehensive approach to evaluating and improving web site security.</i></p> <p>This program accredits merchants and service providers against the Payment Card Industry Data Security Standard through a combination of onsite audits and penetration testing. The program is run on a global basis by MasterCard and all audits and testing must be performed by certified organisations.</p>
<p>Payment Card Industry Data Security Standard (PCI DSS)</p>	<p><i>MasterCard and VISA have aligned both the process and standard for the relative programs.</i></p> <p>MasterCard and VISA had until January 2005 been managing independent compliance programs for their merchants, service providers and acquirers. These programs were designed to promote good practice around the storage and processing of credit card transactions. The programs were focused on the delivery of services via the Internet especially where large numbers of transactions are involved.</p> <p>In February 2005, the technical and compliance validation requirements for VISA Account Information Security (AIS) and the MasterCard Site Data Protection Program (SDP) have been aligned.</p> <p>Later on, the other major payment brands (e.g. American Express, Discover, JCB) joined the PCI DSS scheme.</p>

PCI SSC Roles & Payment Brand Roles

PCI SSC	PCI SSC (Payment Card Industry Security Standards Council) is responsible for the PCI DSS and supporting documents
Payment Brand	<p>Each payment brand develops and maintains its own PCI DSS compliance programmes in accordance with its own security risk management policies.</p> <ul style="list-style-type: none">● American Express: Data Security Operating Standard (DSOP)● Discover: Discover Information Security Compliance (DISC)● JCB: Data Security Program● MasterCard: Site Data Protection (SDP)● Visa USA: Cardholder Information Security Program (CISP)● Other Visa Regions: Account Information Security (AIS) Program <p>All these programmes have now been aligned with PCI DSS.</p> <p>Payment Brand Compliance Programmes include:</p> <ul style="list-style-type: none">● Tracking and enforcement● Penalties, fees, compliance deadlines● Validation process and who needs to validate● Approval and posting of compliant entities● Definition of merchants and service provider levels● Payment brands are also responsible for forensics and response to account data compromises

Selection Criteria & Compliance Reports

VISA's criteria for accreditation Merchants

Level/ Validation action	Selection Criteria	Validate By
Level 1 <ul style="list-style-type: none"> • Annual Onsite Security Audits • Quarterly Network Scan 	Level 1 <ul style="list-style-type: none"> – Any merchant - regardless of acceptance channel - processing over 6,000,000 VISA transactions per year. – Any merchant that has suffered a hack or an attack that resulted in an account data compromise in the last year. – Any merchant identified by another payment card brand as a Level 1. 	<ul style="list-style-type: none"> •Qualified Security Assessor •Internal Auditor •Approved Scanning Vendor
Level 2 <ul style="list-style-type: none"> • Annual Self Assessment Questionnaire • Quarterly Network Scan 	Level 2 <ul style="list-style-type: none"> – Any merchant processing 1,000,000 to 6,000,000 VISA transactions per year. 	<ul style="list-style-type: none"> •Company executive •Approved Scanning Vendor
Level 3 <ul style="list-style-type: none"> • Annual Self Assessment Questionnaire • Quarterly Network Scan 	Level 3 <ul style="list-style-type: none"> – Any e-commerce merchant processing up to 1,000,000 Visa e-commerce transactions per year. 	<ul style="list-style-type: none"> •Company executive •Approved Scanning Vendor
Level 4 <ul style="list-style-type: none"> • Annual Self Assessment Questionnaire (recommended) • Network Scan (recommended) 	Level 4 <ul style="list-style-type: none"> – Any merchant processing less than 20,000 VISA e-commerce transaction per year. – All other merchants processing up to 1,000,000 VISA transaction per year. 	<ul style="list-style-type: none"> •Company executive •Approved Scanning Vendor

Full details of the selection criteria can be found at:

http://www.visaeurope.com/documents/ais/Merchant_levels_and_AIS_compliance_validation.pdf

MasterCard's criteria for accreditation – according to MasterCard UK Merchants

Level/ Validation action	Selection Criteria	Validate By
Level 1 <ul style="list-style-type: none"> • Annual Onsite Security Review • Quarterly Network Security Scan 	Level 1 <ul style="list-style-type: none"> – All merchants, including electronic commerce merchants with more than 6,000,000 total MasterCard transactions annually. – All merchants that experienced an account compromise. – All merchants meeting the Level 1 criteria of a competing payment brand. – Any merchant that MasterCard, at its sole discretion, determines should meet the Level 1 merchant requirements. 	<ul style="list-style-type: none"> • Qualified Security Assessor • Internal Auditor • Approved Scanning Vendor
Level 2 & 3 <ul style="list-style-type: none"> • Annual Self Assessment Questionnaire • Quarterly Network Security Scan 	Level 2 <ul style="list-style-type: none"> – All merchants with annual e-commerce transactions between 150,000 and 6,000,000. – All merchants meeting the Level 2 criteria of a competing payment brand. Level 3 <ul style="list-style-type: none"> – All merchants with annual e-commerce transactions between 20,000 and 150,000. – All merchants meeting the level 3 criteria of a competing payment brand. 	<ul style="list-style-type: none"> • Company executive • Approved Scanning Vendor
Level 4 <ul style="list-style-type: none"> • Annual Self Assessment Questionnaire (recommended) • Quarterly Network Security Scan (recommended) 	Level 4 <ul style="list-style-type: none"> – All other merchants 	<ul style="list-style-type: none"> • Approved Scanning Vendor

Full details of the selection criteria can be found at:

http://www.mastercard.com/uk/merchant/en/security/what_can_do/SDP/merchant/levels.html

MasterCard's criteria for accreditation - according to MasterCard US Merchants

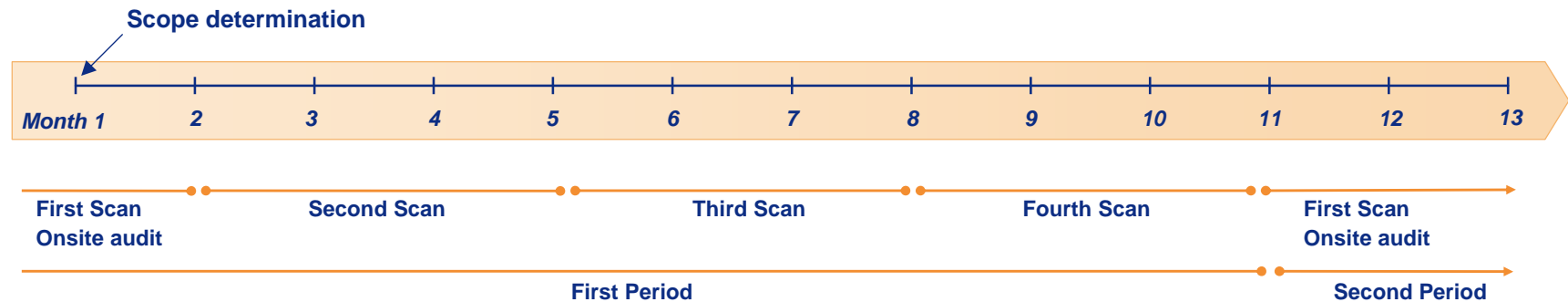
Level/ Validation action	Selection Criteria	Validate By
Level 1 <ul style="list-style-type: none"> • Annual Onsite Security Review • Quarterly Network Security Scan 	Level 1 <ul style="list-style-type: none"> – All merchants, including electronic commerce merchants with more than 6,000,000 total MasterCard transactions annually. – All merchants that experienced an account compromise. – All merchants meeting the Level 1 criteria of a competing payment brand. – Any merchant that MasterCard, at its sole discretion, determines should meet the Level 1 merchant requirements. 	<ul style="list-style-type: none"> • Qualified Security Assessor • Internal Auditor • Approved Scanning Vendor
Level 2 & 3 <ul style="list-style-type: none"> • Annual Self Assessment Questionnaire • Quarterly Network Security Scan 	Level 2 <ul style="list-style-type: none"> – All merchants with annual e-commerce transactions between 1,000,000 and 6,000,000. – All merchants meeting the Level 2 criteria of a competing payment brand. Level 3 <ul style="list-style-type: none"> – All merchants with annual e-commerce transactions between 20,000 and 1,000,000. – All merchants meeting the level 3 criteria of a competing payment brand. 	<ul style="list-style-type: none"> • Company executive • Approved Scanning Vendor
Level 4 <ul style="list-style-type: none"> • Consult Acquirer • Annual Self Assessment Questionnaire • Quarterly Network Security Scan (recommended) 	Level 4 <ul style="list-style-type: none"> – All other merchants 	<ul style="list-style-type: none"> • Company executive • Approved Scanning Vendor

Full details of the selection criteria can be found at:

http://www.mastercard.com/us/sdp/merchants/merchant_levels.html

Wincor Nixdorf CR and KPMG CR's overall approach to the programmes

Current schedule for accreditation



VISA and MasterCard require that all acquirers, merchants and service providers comply with the Payment Card Industry Data Security Standard through their own compliance programmes (Account Information Security, Site Data Protection).

<p>Requirements for compliance</p>	<p>In general, major merchants and all service providers: Annual onsite audits and quarterly scans must be performed by a registered Qualified Security Assessor (or Internal Audit in case of merchants) and Approved Scanning Vendor respectively.</p> <p>In general, medium sized merchants : Quarterly scans must be performed by a registered Approved Scanning Vendor.</p>
---	---

PCI DSS Scoping

Scoping

- The PCI DSS security requirements apply to **all system components**.
- “System components” are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.
- Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
- Applications include all purchased and custom applications, including internal and external (Internet) applications.

Network segmentation

- Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment
- The assessor must verify that the segmentation is adequate to reduce the scope of the audit

PCI DSS Scoping

	Data Element	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	YES	YES
	Cardholder name	YES	YES
	Service Code	YES	YES
	Expiration Date	YES	YES
Sensitive Authentication Data	Full Magnetic Stripe	NO	N/A
	CVC2/CVV2/CID/CAV2	NO	N/A
	PIN / PIN Block	NO	N/A

PCI Data Security Standard Requirements

Build and Maintain a Secure Network

Requirement 1	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5	Use and regularly update anti-virus software
Requirement 6	Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7	Restrict access to cardholder data by business need-to-know
Requirement 8	Assign a unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12	Maintain a policy that addresses information security
----------------	---

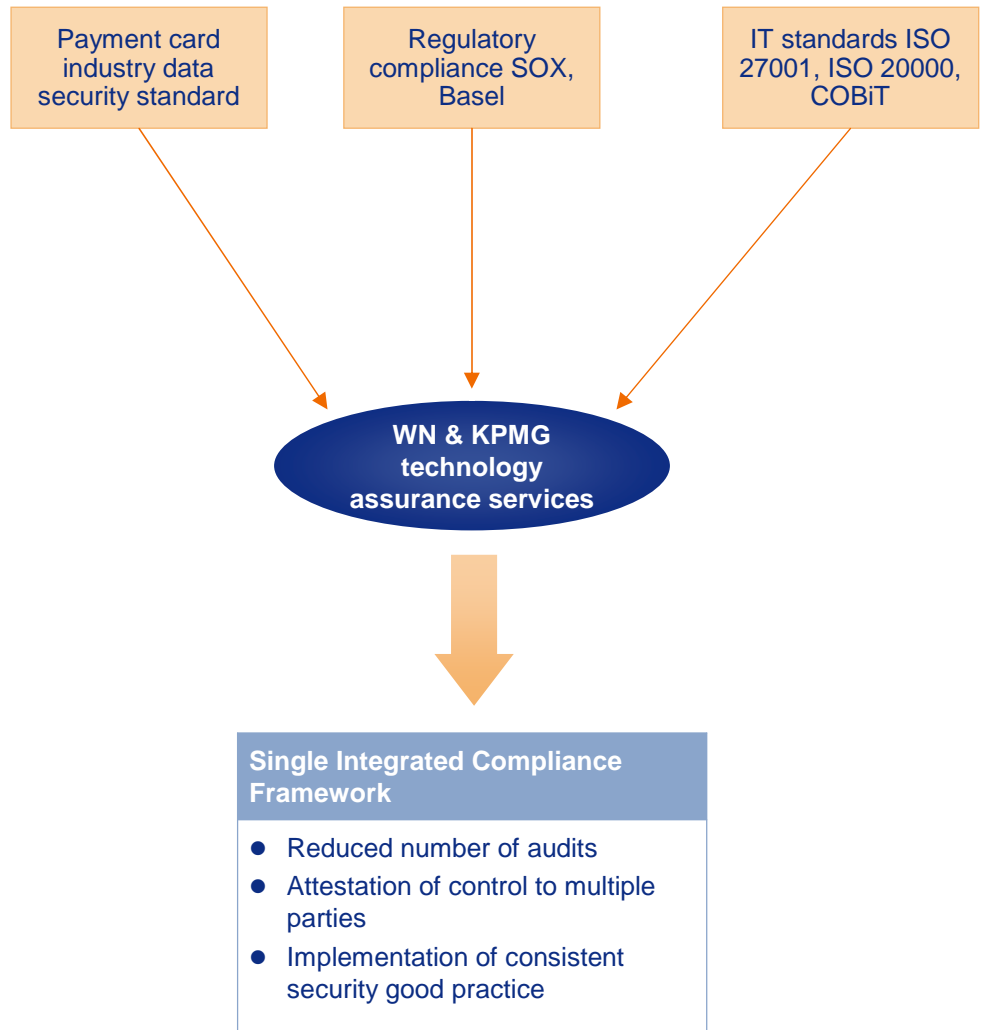
WN CR & KPMG CR approach – on site audit

WN & KPMG's on site audit work will focus on assessing compliance with the Payment Card Industry (PCI) Data Security Standard. Our method of completing the onsite audit is designed to maximise the benefits from the audit, whilst minimising the impact on our clients' business

- We will use approved materials that are designed to achieve compliance with the minimum of effort on client part
- We will augment the reporting mechanism required under the program to provide a client with sufficient details that can be used to meet its own internal compliance requirements
- We will only focus on the systems that are required under the program unless requested by a client
- We will minimise the impact on client's business by maximising the level of integration with existing WN and/or KPMG teams a client may have assisting him and reduce the level in duplication of effort by using information that has already been gathered as part of other WN and/or KPMG engagements

If required, WN & KPMG can supplement the on site audit to provide sufficient evidence to support other regulatory or internal compliance requirements you may have

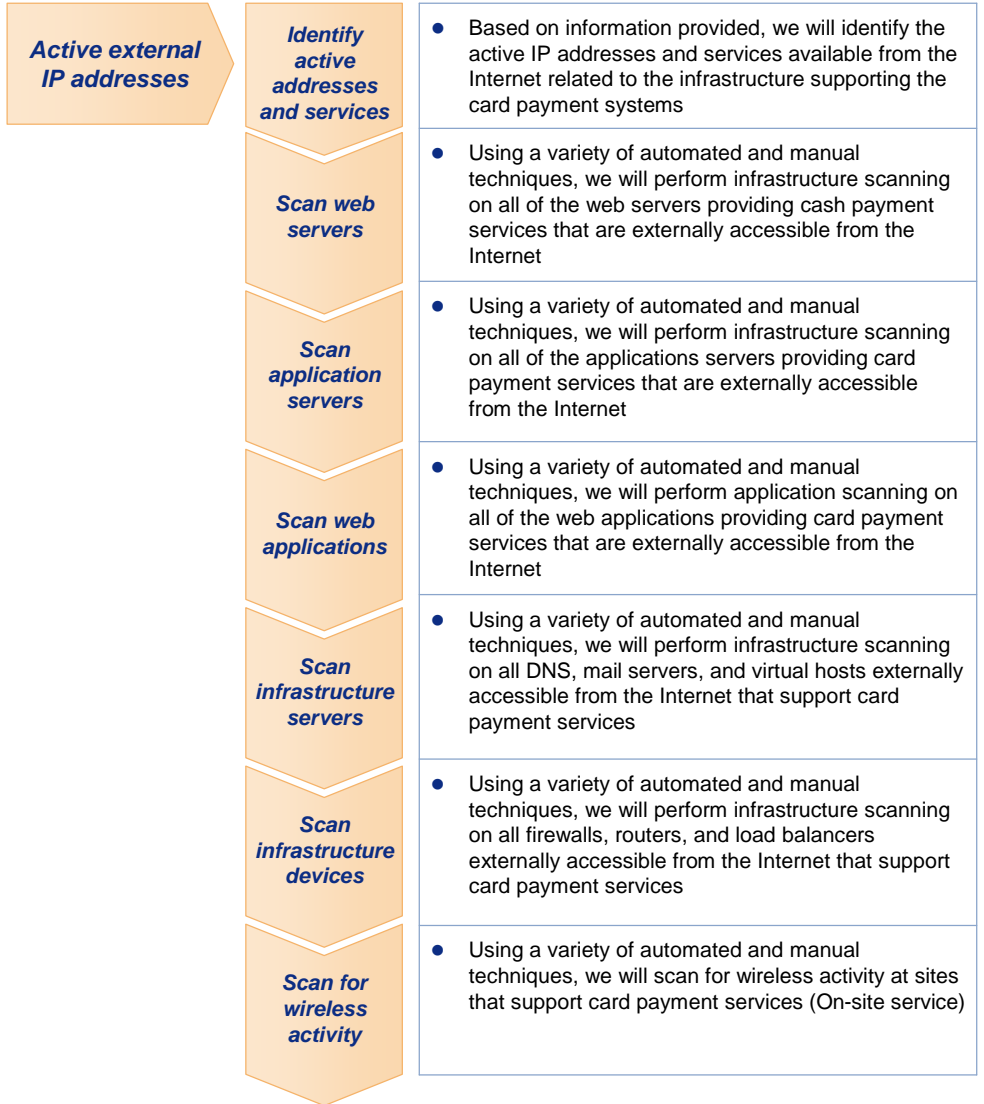
- By using joined WN and KPMG team to assist in multiple auditing activities, a company can achieve cost reductions through economies of scale and a single-audit, multiple-reports approach
- By having a single team associated with your auditing requirements, we can achieve an understanding of your business that promotes an efficient audit process and a collaborative approach to third party attestations



PCI DSS approach – quarterly security scans

PCI approach to security scanning focus on assessing the compliance with Payment Card Industry (PCI) vulnerability assessment requirements

- Only Accredited Scanning Vendors (ASV) are allowed to perform vulnerability scanning and submit reports to PCI
- If required, WN & KPMG can perform a test scan which will help clients to determine whether they are ready for the test performed by an accredited ASV



PCI DSS approach – quarterly security scans (continued)

In order to provide feedback on any vulnerabilities identified, we will report using the PCI levels of risk and map these onto a status mechanism for compliance with the PCI requirements

Level 5 Urgent	<ul style="list-style-type: none"> Trojan Horses, file read and writes exploit, remote command execution 	Level 3 Status	Level 4 Status	Level 1	<ul style="list-style-type: none"> No identified issues
Level 4 Critical	<ul style="list-style-type: none"> Potential Trojan Horses, file read exploit 			Level 2 (in progress)	<ul style="list-style-type: none"> Low/ medium level issues, medium to long term response required
Level 3 High	<ul style="list-style-type: none"> Limited exploit of read, directory browsing and denial of service (DoS) 			Level 3 (in progress)	<ul style="list-style-type: none"> Few high level issues and some medium/low level issues, short to medium term response required
Level 2 Medium	<ul style="list-style-type: none"> Sensitive configuration information can be obtained by hackers 	Level 2 Status		Level 4 (failed)	<ul style="list-style-type: none"> Multiple high level issues, short term response required
Level 1 Low	<ul style="list-style-type: none"> Information can be obtained by hackers on configuration 				

PCI DSS Versions and PA DSS

PCI DSS versions

- In October 2008 new version of PCI DSS was released. New version 1.2 contains several clarifications of the requirements and introduces some new or tightens existing ones.
- The nature of requirements has not changed, changes to the requirements were made to:
 - tighten wireless security,
 - incorporate messaging technologies,
 - tighten antivirus protection,
 - make code reviews or implementation of web-application firewall mandatory,
 - tighten media handling procedures.
- PCI DSS 1.2 also contains forms for reporting compliance and information to fulfilling self-assessment form.

PA DSS

- Payment Application Data Security Standard (PA-DSS) is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. In-house payment applications developed by merchants or service providers that are not sold to a third party are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI DSS.

Security Breaches and Vulnerability Experiences

PCI environment

PCI environment

- Increased regulatory pressure to address security risk
 - including activities of European Union with regard to SEPA
- Emerging technologies and products introduce new security risks (pre-paid cards, contact-less cards)
- Frauds are committed through international organized crime
- Lack of international cooperation for card fraudster arresting and prosecuting
- Significant increase of Card-Not-Present fraudulent transactions and phishing activities
- Processors and service providers being aggressively targeted through lack of security at internet access points
- Attacks against the application layer are increasing
- Insider threats are a recognized risk



There has been a need for a security standard enforced by a powerful entity.

Security Vulnerabilities and Risks

Vulnerabilities

- Improper storing of data
- Insecure applications
- Insecure e-commerce sites
- No segmentation and/or firewall
- Un-patched systems and/or default configuration
- No logging
- Insecure wireless access point
- Default passwords
- No intrusion monitoring
- Unsecured point of sale technology

Risks

- Compromise disclosure
- Financial liabilities and fees
- Litigation
- Loss of confidence
- Loss of reputation
- Government intervention / regulation

Security Breaches examples

RBS WorldPay Announces Compromise of Data Security

Source: <http://www.tmcnet.com/submit/2008/12/23/3875815.htm> (December 2008)

Data taken, company says

Source: <http://www.canada.com/vancouver/news/westcoastnews/story.html?id=055fa12a-2bca-4804-9bef-a44eee60de5f> (November 2008)

Report: Montgomery Ward fails to alert victims of breach

Source: <http://www.scmagazineus.com/Montgomery-Wards-online-retail-data-breach/article/111922/> (June 2008)

Supermarket data breach exposes more than 4 million accounts

Source: http://news.cnet.com/8301-10784_3-9896217-7.html?tag=mncol;txt (March 2008)

Program Documentation

Official PCI DSS Documentation	Payment Card Industry Data Security Standard 1.2 https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf Payment Card Industry Security Scanning Procedures https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf
VISA Documentation	Information about AIS process for VISA http://www.visaeurope.com/aboutvisa/security/ais/aisprogramme.jsp VISA SPECIFIC: Selection Criteria for Merchants and Service Providers http://www.visaeurope.com/documents/ais/Merchant_levels_and_AIS_compliance_validation.pdf http://www.visaeurope.com/documents/ais/service_provider_validation_requirements.pdf
MasterCard Documentation	Site Data Protection Program http://www.mastercard.com/us/merchant/security/sdp_program.html MC SPECIFIC: Selection Criteria for Merchants and Service Providers http://www.mastercard.com/us/sdp/merchants/merchant_levels.html http://www.mastercard.com/us/sdp/serviceproviders/serviceprovider_levels.html

WN CR and KPMG CR PCI team

- We will use a team of staff which includes personnel with a mix of skills to match PCI's requirements of the required audits. Wherever possible we will engage with you at a local practice level in order to better understand the local issues relevant to your organisation.
- The overall management and quality assurance of the on-site reviews as well as remote scanning reports will be performed by **Tomas Kudelka**.



Name	• Tomas Kudelka, CISA, CISM, CGEIT, QSA
Position	• Senior Manager at KPMG Czech Republic
Experience	<ul style="list-style-type: none"> • Tomas Kudelka joined KPMG in 1999. Currently Tomas is heading up KPMG IT Advisory team in the Czech Republic. In 2004-2005 he has been on secondment in KPMG UK. His main specialization is information security • Tomas has been involved in various engagements in this area including PKI and chip card implementation, penetration testing and security policy developments. • Tomas has been involved in development of various security policies and programs for MasterCard International. • Form 2005 Tomas has been working on PCI security reviews helping clients to implement PCI DSS security requirements.
Contact	• tkudelka@kpmg.cz, Tel: +420 222 123 388, Mobile: +420 724 244 944

- The key Wincor Nixdorf contact is **Michal Prazny**.



Name	• Michal Prazny
Position	• Director at Wincor Nixdorf Czech Republic
Experience	<ul style="list-style-type: none"> • Michal Prazny joined Wincor Nixdorf in 2000. Currently Michal is leading Wincor Nixdorf CZ application development and IT operation department • Michal is responsible for <ul style="list-style-type: none"> • projects in EFT and ATM transaction area • PCI DSS implementation in Wincor Nixdorf CZ • Wincor Nixdorf CZ PCI SSC QSA membership
Contact	• michal.prazny@wincor-nixdorf.com, Tel: +420 233 034 152, Mobile: +420 603 459 515