

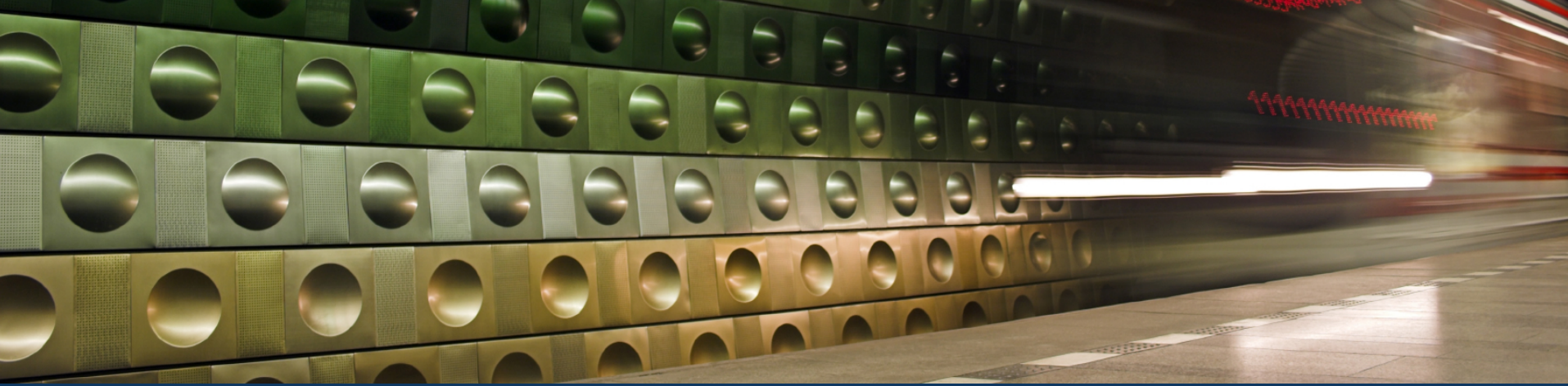


1. PCI DSS – 2010 & Beyond

“We are not saying just comply with our standard, it is the building blocks and a good basis for security to build a good level of security and from that, a good level of compliance will follow.”

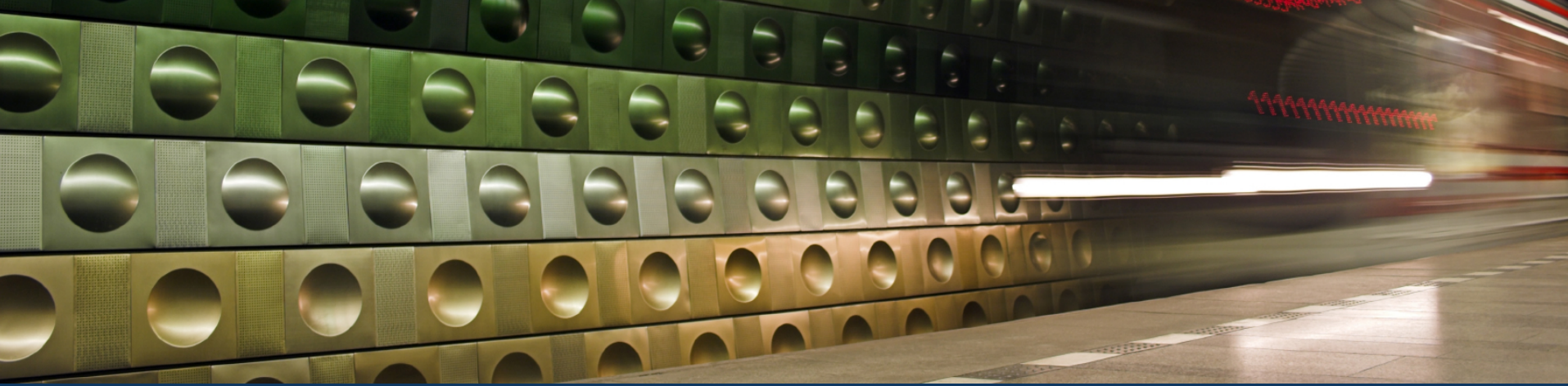
Jeremy King

*Newly Appointed European Director
PCI Security Standards Council*



2. Working with your QSA

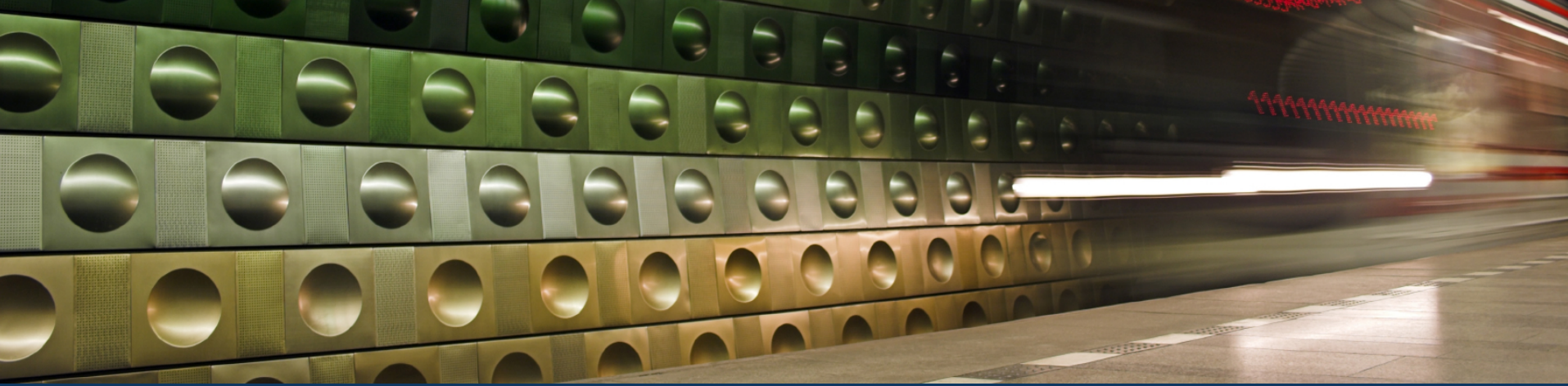
- Many organisations are now looking at PCI as BAU practice
- Many however are still working on getting to the first fence and achieving compliance with the PCI DSS
- Other organisations have been working towards compliance for a long time and have a fully mapped programme of work spanning several years.
- Some organisations have worked with several different QSAs and have still not achieved compliance.....why not?



2. Working with your QSA

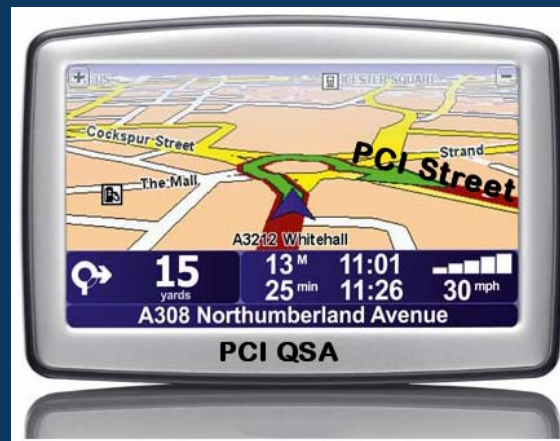
- What is the role of the QSA?
 - Auditor or Mentor or a bit of both?
- Read the Requirements and Security Assessment Procedures carefully and see how many times the word AUDIT is used...
- The QSA should be working with you to achieve compliance and identify ways in which improvements in security practice can be made.





2. Working with your QSA

- The QSA should give you advice that helps you maintain compliance going forward.





3. Getting Value from your PCI project

- A PCI DSS assessment should not purely be an annual tick box exercise.
- However, just like an MOT, a PCI DSS assessment is only a “snapshot” of an environment at a given time.
- So what does that mean ?

3. Getting Value from your PCI project

- Your car could pass its MOT in the morning and be made un-roadworthy on the way home



3. Getting Value from your PCI project

- PCI DSS is the same.
- You may only be one ill conceived change control request away from a non-compliance.
- Security must be a 24 / 7 / 365 business as usual process.





3. Getting Value from your PCI project

- Some thoughts from a QSA:
- It is frequently useful to have a separate list of mandatory requirements picked up as part of the PCI review and also to document the aspirational improvements relating to Information Security in general;
- The DSS is only a MINIMUM set of controls after all;
- Know your threat profile and exert maximum effort in these areas first;
- Speak to your Acquiring Bank – they will be pleased to hear from you.



3. Getting Value from your PCI project

- Be mindful of changes to relevant standards:
 - PCI DSS V 2.0 is now published
 - OWASP Top Ten – was updated in April 2010. This will have consequences with regards to PCI requirement 6.5 – “To Develop web applications in accordance with industry recognised secure coding guidelines.”
- So.....isn't this a lot of needless effort?



3. Getting Value from your PCI project

- Why bother with PCI DSS?
- We all know the usual answers....BUT have you considered:
 - It can be a very useful tool to promote best practice within an organisation
 - Ability to secure budgets for practices that have remained aspirational until now
 - Add value to an organisation in much the same way as an ISO 27001 accreditation would
 - Build upon the baseline provided by the PCI DSS for the CDE for other parts of the organisation.



4. Quality Assurance and PCI QSAs

- If you are having an onsite assessment, you will no doubt have heard of the “Scoring Matrix”
- Some background – many assessments were merely scratching the surface.
 - We have seen large corporates with multiple acquisition channels that have assessments completed by QSAs in less than a week.
 - This approach obviously cannot be a proper sample of the environment



4. Quality Assurance and PCI QSAs

- The scoring matrix gives set guidelines for what the QSA must assess and what needs to be included in the report.
- When the PCI Council released statistics on the Quality Assurance process at the end of 2009, the results were surprising:



4. Quality Assurance and PCI QSAs

- 144 ROCs had been reviewed by the PCI SSC QA workgroup
- The average score was 68% - the lowest passing score is 75%
- The Council aimed to sample 50-60 QSAs in 2009
- The reviews were for ROCs that had been completed some time ago, so perhaps not an accurate reflection of current working practice or experiences.
- Even so.....a more uniform approach was required.



4. Quality Assurance and PCI QSAs

- The Scoring Matrix :

v1.2 PCI-DSS Report on Compliance Test Procedures Score Sheet

v1.2 PCI DSS Requirement	Testing Procedure	Verified by Observation of system settings or configuration files	Verified by review of documentation	Verified by Interview	Verified by observation of process, action or state	Sampling Specified	Verified by network traffic monitoring	Points	N/A Points	Section Points
9.9.1 Properly maintain Inventory logs of all media and conduct media Inventories at least annually.	9.9.1 Obtain and review the media Inventory log to verify that periodic media inventories are performed at least annually.		1		1			2	0	
5.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	5.10 Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:		1					1	0	



4. Quality Assurance and PCI QSAs

- A subsequent entry from the Report on Compliance:

<p>9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.</p>	<p>9.9.1 Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.</p>	<p>✓</p>		<p>Verified by review of Firesafe and Inventory procedure documentation that the media inventory log is checked and validated on a quarterly basis. This is documented in the policy and also scheduled in the security events diary.</p> <p>Verified by review of the media tracking process and associated documentation that that a <u>current inventory log</u> is in place and checks are made on a regular basis to ensure it is accurate. Evidence of the most recent inventory shows that it was completed in the last 30 days.</p>
---	---	----------	--	---



4. Quality Assurance and PCI QSAs

- The PCI SSC Scoring Matrix may also be a useful tool for organisations that are not having a full QSA driven assessment or want to conduct their own in house “pre-assessment”.
- Sampling during the assessment can be used but must be justified – it is only useful in an environment where conformity can be assured (may be very suitable for Retail POS estates).



5. PCI Council News

- The PCI SSC has created a new post – “European Director” - which will report back to the US. This gives the UK in particular a very strong voice as the position has been filled by Jeremy King, formerly of MasterCard.
- PCI SSC have launched a new, easier to use website with more information, updated FAQ’s and a document library section.
- A new version of the standard was released in October – v2.0
- The SAQs have also been updated – with a new one for Virtual Terminals
- What does this hold in store?



5. PCI Council News

- The new version is v2.0 and is available now from PCI SSC
- Both v 1.2 and v 2.0 are currently available. You can address either standard at the moment but v1.2 will fall away at the end of 2011.
- Speak to your acquirer if you are unsure which one to use.
- Many people are concerned about the advent of a new set of requirements and what it will mean to them.
- Is this a case of moving goalposts?



5. PCI Council News

- In order to stay effective in the battle against card fraud, trends in data compromises are analysed and help to drive forward the evolution of the standard.
- There will always be some leeway in the timescales for organisation upgrading to a new version of the PCI DSS.
- The schemes and the PCI Council recognise this and will be able to give guidance on compliance with any new version of a standard.



5. PCI Council News

- Jeremy King, the New PCI European director said recently:
 - *"I shall be working with the card brands and the acquirers to filter down the relevant and correct information so they understand the timescales they need to work to."*



5. PCI Council News

- Some of the areas that have been revised as part of the October update of the standard:
 - Lifecycle of the PCI DSS
 - Scope of Assessment
 - Using PAN to define the scope
 - Virtualisation (req 2.2.1)
 - Risk based approach to addressing vulnerabilities
 - New SAQ documents published to reflect the updated standard – also New SAQ C – VT published.

SRM



5. PCI Council News

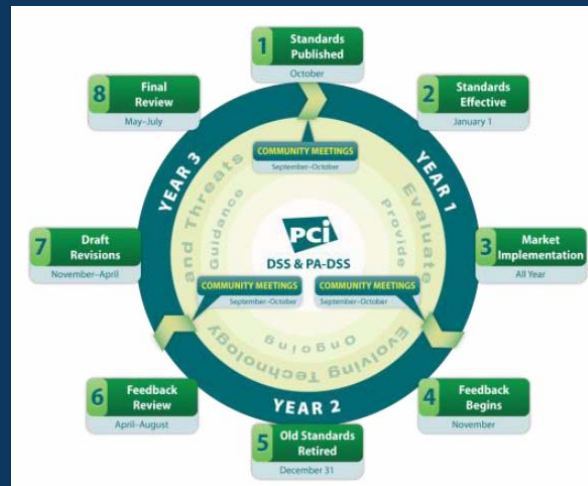
- Mainly clarifications and minor changes of wording.
- No major new requirements have been introduced.





5. PCI Council News

- Lifecycle of the PCI DSS :
 - The standard has moved from a 2 year lifecycle to 3 years





5. PCI Council News

- Scope of Assessment:
 - Clarifications published around how to scope a CDE;
 - The key is to produce good data flow diagrams
 - Document all card data Locations, networks, processes;
 - Legacy data storage can be an issue, so be sure to include all data repositories even if they are dormant.



5. PCI Council News

- Using PAN to define the scope
 - V2.0 has updated wording in the opening section
 - “PCI DSS requirements are applicable if a PAN is stored, processed or transmitted”;
 - Requirements 3.3 and 3.4 have been updated for clarity;
 - Extra guidance included around Hashed & Truncated PAN data;
 - PAN data is frequently stored for marketing or statistical purposes – this should not be overlooked when scoping the CDE;



5. PCI Council News

- Virtualisation
 - v2.0 clarifies intent regarding “One primary function per server”
 - PCI SIG has been working on this for some time;
 - Have been putting together a matrix for virtualized environment and mapped PCI controls onto this – due to be published early 2011;
 - Key is to have good management;
 - Dormant environments must also be scrutinized as they can easily become out of date (patches etc.).



5. PCI Council News

- Virtualisation
 - The management level must always be in scope if any CHD held;
 - Traditional defences may not be sufficient;
 - Effective segmentation may be just as applicable within the VM environment as in a traditional architecture;
 - Cloud computing – in a truly remote system, scoping will need to be carefully considered.



5. PCI Council News

- Virtualisation – Mapping to the PCI DSS

Requirement 1: Install and maintain a firewall configuration to protect cardholder data								
			Client / Endpoint Virtualization		Network Virtualization		Datacenter / Cloud Virtualization	
Section	Description	Virtualization Applies	Special Requirements for Virtualization	Special Testing Procedures for Virtualization	Special Requirements for Virtualization	Special Testing Procedures for Virtualization	Special Requirements for Virtualization	Special Testing Procedures for Virtualization
1.1	Establish firewall and router configuration standards that include the following:	X	Virtual firewalls and routers that exist within client/endpoint components are in-scope.		Virtual firewalls and routers that exist within network components are in-scope.	While this is the same as in physical, specific issues need be called out with virtual networks due to the fact that traffic may never hit the physical network. This needs to be audited to make sure same level of network segmentation is achieved in the virtual environment.	Virtual firewalls and routers that exist within server components are in-scope.	While this is the same as in physical, specific issues need be called out with virtual networks due to the fact that traffic may never hit the physical network. This needs to be audited to make sure same level of network segmentation is achieved in the virtual environment.
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	X	Need to explicitly call out the need to monitor VM to VM traffic flows that never make it out to the physical network.		Need to explicitly call out the need to monitor VM to VM traffic flows that never make it out to the physical network.		Need to explicitly call out the need to monitor VM to VM traffic flows that never make it out to the physical network.	
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	X	Need to document intrahost data flows.				Need to document intrahost data flows.	



5. PCI Council News

- Risk based approach to addressing vulnerabilities
 - Update to requirement 6.2 to include risk based assessment;
 - Processes should be in place to rank vulnerabilities according to risk:
 - Guidance provided on how to assign risk rankings
 - This process should be included in test procedures.
 - NOTE – this is considered best practice until June 30th 2012, after which time it becomes **MANDATORY**.



5. PCI Council News

- All New SAQs published.
 - These now include the minor changes and clarifications provided in v2.0;
 - In addition, a new SAQ C has been issued to cater for Virtual Terminal environments;
 - This is not intended for ecommerce merchants – rather those that use a virtual terminal or web portal to key MOTO transactions, with no electronic Card data storage.
 - SAQ C – VT.



5. PCI Council News



Payment Card Industry (PCI)
Data Security Standard
**Self-Assessment Questionnaire C-VT
and Attestation of Compliance**

**Web-Based Virtual Terminal, No Electronic
Cardholder Data Storage**

Version 2.0
October 2010



6. Final Thought.....

“Continuous effort – not strength or intelligence – is the key to unlocking our potential”

Winston Churchill

Thank You.

Head Office: Fabriam Centre, Cobalt Business Exchange, Cobalt Park Way, Newcastle upon Tyne. NE28 9NZ.
Company registration: 3950239.

Telephone: 08450 212 151
Fax: 08452 808 182

© 2010 Security Risk Management Ltd.

www.srm-solutions.com