Req.	PCI DSS Update	Purpose / Need Addressed	Froud’s Comments
1	Have a current diagram that shows cardholder data flows.	To clarify that documented cardholder data flows are an important component of network diagrams.	The creation and maintenance of both network and data flow diagrams is a business requirement, not just a PCI one. Any organisation that has been through PCI more than once, and has a decent QSA, should not need this explained. Visio has the ability to ‘layer’ one diagram on top of the other making this easy to fulfill: 1. Layer 1 – A diagram that shows both the network / VLAN architecture, and a representation of the systems within each subnet (web server, app server etc.). This is the basic detail that goes into the RoC. 2. Layer 2 – Detail of all IP addresses, VLAN tags, hostnames etc. Basically anything that allows a network admins, system admin, and assessors alike to validate the firewall / router rule sets at the level of detail described in DSS Req. 1.X. 3. Layer 3 – As many layers as represent the application flows through the network. If you have multiple apps, you will have multiple layer 3s. These flows should have, for example, numbered arrows that correspond to the data flow narratives required in the RoC Executive Summary. 4. Layer 4 – Probably don’t need this in most environments, but some organization like to show application / location / system inter-dependencies separately, the layering approach makes this very simple. Some networks are extremely complex, so break them down into logical units, and if even that is too much, your network is probably too complex, and more than likely, unmanageable in a way that maximises efficiency and security. There are a number of network discovery / mapping / enumeration tools out there which should be run on a regular basis to ensure that the network infrastructure is what, and DOING what it’s supposed to. Finally, if you can build your network diagrams from your Asset Management system, you are WAY ahead of the game.

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
2	Maintain an inventory of system components in scope for PCI DSS.	To support effective scoping practices.	Before a QSA shows up on-site to begin the assessment process, they should have asked you for a minimum of 3 things, and a 4th if they're really good: 1. Network Diagram(s) – How can you possibly begin an assessment until you have a basic understanding of what you're looking at? 2. Data Flow Diagram(s) + Detailed Narrative(s) – Again, if YOU don't understand how your applications work, how can the assessor possibly do their job? If you have a decent QSA, they will provide examples of what this stuff should look like, and if necessary, conduct pre-assessment workshops to help you put it together. 3. Asset Inventory – This is a fundamental business practice and a foundation of ANY security programme, not just PCI. You can't manage what you can't measure is one thing, if you have no asset inventory you have no idea what you're trying TO manage in the first place. 4. List of Stakeholders – There's no point in a QSA coming on-site if no-one has any idea who can answer the questions. A good QSA will require a full agenda before coming on-site, and will send all relevant stakeholders a detailed list of all points of action. It is the organisation's responsibility to ensure that the right people are put in front of the QSA. These 3 - 4 FUNDAMENTALS have not changed since DSS v1.0, and if you want to ever do security properly, you'll need an accurate asset management system to do the pre-requisite Risk Assessment and Controls Gap Analysis. If you hired a good QSA, and not just the cheapest, all of this should have been explained during the sales process, and again during the initial pre-assessment orientation. If you're still fumbling with this, or if you see this requirement as an issue for your next assessment, change your QSA.
5	Evaluate evolving malware threats for systems not commonly affected by malware.	To promote ongoing awareness and due diligence to protect systems from malware.	This requirement, and the one below for Req. 6, are not separate, and even though Requirement 5 is ABOUT anti-virus (a/v), it's not the INTENT of it. At least it shouldn't be.

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
			Neither of these requirements start with malware or threats, they START with your configuration standards, evolve through your Risk Management processes (which is what Req. 6 alludes to), and are then base-lined and monitored through your scanning / pen testing / code reviews (Req. 11), and your logging / alerting / incident response (Reqs. 10, and 9 respectively). If you have done, or are thinking of doing, any of the following, you have missed the point; 1. Installed a completely stand-alone anti-virus system for Windows separate from any review for relevance or risk. 2. Retrofit ClamAV on a *nix / nux system just to stop incompetent QSAs from asking silly questions. 3. Hoodwinked your QSA into thinking you have a/v on an AS/400 or mainframe. Hopefully v3.0 of the DSS will clarify that it's not a/v you need, it's an understanding of what your systems SHOULD look and behave like, and the ability to either a) prevent changes, or b) detect changes and react quickly enough to prevent real damage. That's the intent. a/v is increasingly incapable of doing this, and while it may still be of some use (for Windows anyway), what it really means is that you need to stop relying on additional technology to solve your PCI challenges. If you were doing security properly, you would be compliant with v.2.0, and would automatically be compliant with v3.0 and ANY other compliance / regulation / standard out there.
6	Update list of common vulnerabilities in alignment with OWASP, NIST, SANS, etc., for inclusion in secure coding practices.	To keep current with emerging threats.	Per Req. 5 above, you can keep as up to date with emerging threats as much as you like, but if you don't know whether or not the threat is RELEVANT, you are wasting your time. Further, if you have no understanding of the possible IMPACT of the threat, your reaction to the threat may be poorly rated, prioritized, and effected. For example; Threat A is released, what's your first action? If your first

Req.	PCI DSS Update	Purpose / Need Addressed	Froud’s Comments
			action is to compare the threat to your asset database to determine relevance, you’ve met this Req. However, if your first action is to initiate your patching cycle, you have missed the point. Feeds into your Vulnerability Management Programme (which is what this is) do not stop at “OWASP, NIST, SANS, etc.”, they include every vendor from whom you have purchased servers, software, firewalls, routers, databases and so on. It also VERY closely integrates the results your scanning, penetration testing results, code review processes. Finally, all of this (and more) feeds back into your configuration standards and asset inventory in order to close the loop on this iteration of the ongoing cycle.
8	Security considerations for authentication mechanisms such as physical security tokens, smart cards, and certificates.	To address feedback that requirements for securing authentication methods other than passwords need to be included.	This has always been implied, and has always been the intent. You never HAD to have passwords, as long as what you WERE doing is as strong, or stronger.
9	Protect POS terminals and devices from tampering or substitution.	To address need for physical security of payment terminals.	There has always been an enormous grey area on whether or not the POS terminals should be included in the PCI assessment. The answer is yes, they should, but because the PCI DSS did not specifically address it, and there were the PA-DSS / PTS standards on the side, this was largely ignored. The diagram showing the integration of the 3 standards has, until now apparently, been mostly lip-service, so it’s good to see that the integration is finally being addressed. ‘Protection from ‘tampering’ is pushing for the use of PTS compliant terminals only, and ‘substitution’ is pushing for ‘automated Terminal Estate Management’ (TEM), but neither of these things can be a requirement with the vast quantity of legacy systems still not at their End of Life (EoL). This requirement can be met with physical controls and manual processes, but that is far from ideal.

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
11	Implement a methodology for penetration testing, and perform penetration tests to verify that the segmentation methods are operational and effective.	To address requests for more details for penetration tests, and for more stringent scoping verification.	First, if your pentest provider tries to use this updated requirement to sell you more services, fire them. This is not about increasing the AMOUNT of pentesting you perform, it's about performing the RIGHT pentests to meet the intent of the requirements. However, if YOU cheap-out on your choice of pentesting company, or try to do it yourselves without fully qualified internal resources - just to save money and get though your PCI assessment - you deserve to be hacked. Pentesting is a critical aspect of every good practice security programme and is not an area for making savings. Ever. There has been confusion on where exactly a pentester should sit while conducting an internal test. The answer has always been; where anyone can sit who has access to the Cardholder Data Environment (CDE). You do NOT have to open the firewalls to his/her device, and you certainly don't have to provide admin credentials. Basically just pretend they are a bad guy who plugged into your network, what damage can they do? From the outside, that's even easier, just provide your PCI relevant IP ranges, it's up to them to scope it correctly. The issue here is that the scoping exercise has never been conducted properly, and the firewall rule–set reviews are not always conducted by networking experts (blame the QSA training for that one). If you have accurate network and data flow diagrams, full understanding of your firewall ingress / egress filtering, and your access control mechanisms throughout your enterprise, this exercise should be fairly simple. Sure, some form of Data Loss Prevention (DLP) mechanism would help, but until that's spelled out as a requirement (like firewalls, IDS/IPS, WAF, etc.) few organisations will make the expense. If the QSA does their job properly, this requirement should not be an issue.
12	Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity.	To address feedback from the Third Party Security Assurance SIG.	Bottom line; you can outsource almost every FUNCTION of PCI to 3rd parties / service providers, and even some of the accountability, but you can NEVER outsource the responsibility. SOMEONE has to answer the

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
	Service providers to acknowledge responsibility for maintaining applicable PCI DSS requirements.		questions, if not you, then whom? For example; if you outsource the installation, management, maintenance, and monitoring of your firewalls to an MSS, but you will ALWAS own the rule sets, the policies, and your part of the change control process. Your MSS provider has 2 choices; be PCI compliant for the services they are providing to you, or they can go through an assessment every year against YOUR Report on Compliance. There has never been a loophole here if your QSA knew what they were doing, but unfortunately the language related to 12.8.X was too vague and open to MIS-interpretation. Vendor Management and Vendor Due Diligence are notoriously lax in most organisations, and even those processes related to banking and finance are often run by departments who have no concept of what they are asking, the answers they receive, or of what is truly important. I can foresee a great deal of pain on the side of Service Providers who are now going to be asked to provide a ton of additional evidence related to 12.8.X when, in theory, it was the client's due diligence process that was at fault. Retrofitting the new 12.8.X requirements into existing service contracts / SLAs / MSA is simply not going to happen, but any organization that does not now FIX their vendor management processes is going to be in a world of pain down the road.
General	Clarified that sensitive authentication data must not be stored after authorization even if PAN is not present.	To ensure better understanding of protection of sensitive authentication data.	While I can understand why organisations would question this, it just means that any application that DOES this is probably too old to be business viable, let alone PCI compliant. Acquirers used to require all sorts of retention and 'PCI no-no' processes, but have not done so for MANY years. You don't need full PAN for settlement, your don't need CVV for preferred interchange rates on recurring payment and so on. Trying to get out of complying with this requirement just suggests that you want to continue to use applications that have functionality outside of their actual requirements. All security starts with no functionality and no access and goes up from there, not the other way around.

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
General	Added guidance for implementing security into business-as-usual (BAU) activities and best practices for maintaining on-going PCI DSS compliance.	To address compromises where the organization had been PCI DSS compliant but did not maintain that status. Recommendations focus on helping organizations take a proactive approach to protect cardholder data that focuses on security, not compliance, and makes PCI DSS a business-as-usual practice.	Too little too late, and once again, completely misses the point. How can there be talk of Business as Usual when the DSS misses out almost every step that goes before it, focuses only on cardholder data, and apparently fails to appreciate that all of this is based on a technology that's over SIXTY years old?; the credit card number. Why would any organization make the effort to ensure PCI compliance is Business as Usual, when, by my reckoning, card numbers will be steadily phased out by innovations in payment methods? Security follows these Core Concepts, and in this order for newly initiated programmes; 1. Security Core Concept 1: Risk Assessment / Business Impact Analysis 2. Security Core Concept 2: Security Control Choice & Implementation 3. Security Core Concept 3: Security Management Systems 4. Security Core Concept 4: Governance & Change Control 5. Security Core Concept 5: Incident Response (IR) & Disaster Recovery (DR) 6. Security Core Concept 6: Business Continuity Management (BCM) & Business As Usual (BAU) So yes, PCI requires; • a Risk Assessment, but it only has to cover the PCI relevant infrastructure and processes • security controls (that's pretty much all it is), but they are a bare minimum set and, again, it's only PCI relevant systems • an incident response programme, but it only relevant to cardholder data, and NOT business saving disaster recovery • change control, but they make no mention of how it's run properly i.e. though Governance So how do you get to Business as Usual when the DSS makes no mention whatsoever of Business Continuity Management?

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
General	Added guidance for all requirements with content from the former Navigating PCI DSS Guide.	To assist understanding of security objectives and intent of each requirement.	This should have always been available from the QSAs, but to my knowledge, this is still very much missing from the QSA curriculum. Anyone can read the CISA / CISM / CISSP books and pass the multiple choice questions, but it takes a real consultant to both explain the intent of PCI, and, perhaps more importantly, fit that in to their client's business needs, not the other way around. I'm glad that this is a developing process, all we need now is a way to develop the QSAs along with it.
General	ROC reporting section relocated to a separate reporting template.	To simplify and streamline the reporting process.	I can't see how this streamlines things if the actual CONTENT of the separate reports is unchanged, but I cannot comment further.
General	Enhanced testing procedures to clarify the level of validation expected for each requirement.	To put more emphasis on the quality and consistency of assessments.	About time! However, unless the language of the new Testing Procedures actually matches the reporting requirements, there will continue to be confusion and inconsistency. For example, the current testing procedure for the PCI Req. 3.5.1 is; "*Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.*" Yet if you don't write something like; "*[QSA Company] observed settings and configurations, identified locations of cryptographic key storage, reviewed user access lists and verified that access to keys is restricted to the fewest number of custodians necessary*.", then detail the encryption solution(s), clarify the number of key custodians AND detail the configurations examined, you've failed the QA scoring requirements. If you want assessors to 'examine', 'verify', 'review', 'interview', 'confirm', 'observe', 'identify' and so on, put THAT in the testing procedure, not the QA documents. Better yet, teach the QSAs how to actually validate properly instead of focusing on merchant and service provider levels.

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
Multiple	Incorporate security policy/procedure requirements into each requirement (replaces former 12.1.1 and 12.2).	To address feedback that policy topics should more closely align with the related technical PCI DSS requirement.	Good, but I would have loved to see each policy requirement have 2 aspects; 1. The paperwork, and; 2. What the QSA did to validate the policies are actually enforced, and not just 'read and understood'. Far too often the policy and procedure requirements of the DSS (roughly 40% of the entire standard) are seen as a paperwork-only exercise, with little understanding - and less caring - that policies are a foundation of security every bit as important as management buy-in. Which reminds me, where's the emphasis on management accountability for a proper security culture?
2	Clarified that changing default passwords is required for application/service accounts as well as user accounts.	To address gaps in basic password security practices that are leading to compromises.	This is too depressing for words, and not in any way a deficiency in the DSS itself. Any organization that does not do this needs far more than PCI to fix what's broken. The fact that the SSC has to put this in as a more specific requirement just goes to show how much even minimalist standards like the DSS are absolutely necessary.
3	Provided flexibility with more options for secure storage of cryptographic keys, and clarified principles of split knowledge and dual control.	To clarify common misunderstandings about key management.	No comment, encryption is not my forte, but every QSA should understand the need for split knowledge and dual control, and not just in encryption scenarios.
8	Provided increased flexibility in password strength and complexity to allow for variations that are equivalent. Revised password policies to include guidance for users on	To address feedback on improving password security. Changes focus on increased flexibility and user guidance rather than new requirements.	Working out the strength of passwords based upon all their variables is mathematics I will never understand, nor want to for that matter. However, it must be relatively simple surely to put together a matrix of equivalents? e.g. 6 characters + alpha-numeric + change every 60 days = 7 character + alpha-nonstandard + change every 90 days

Req.	PCI DSS Update	Purpose / Need Addressed	Froud's Comments
	choosing strong passwords, protecting their credentials, and changing passwords upon suspicion of compromise.		Bad example, but I think I make the point.
10	Clarified the intent and scope of daily log reviews.	To help entities focus log-review efforts on identifying suspicious activity and allow flexibility for review of less-critical logs events, as defined by the entity's risk management strategy.	This was never about daily REVIEW of log files, it was always about recording the logs, then ALERTING on things you should not see. No-one, I repeat no-one, is able to review a log file manually and do the job properly, and it should never have been offered as an option in the standard. The only way you can comply with sections 10.5.X and 10.6.b is to have a centralized log server of some sort, and automated scripts looking for anomalies. Faking your way past an assessor by describing your manual review process is about as much use to your business as hubcaps on a tractor. It's actually irresponsible. I'm not saying you have to go out and spend tens of thousands on an ArcSight solution, there are many options out there from basic appliances to full outsourcing. Whatever your choice, make sure it's appropriate to your business, ALL of your business, not just the PCI part. There are two reasons to log and monitor: 1) to pro-actively monitor system output to ensure normal operation, and 2) to record everything that happened in case you need to recreate an incident if things went horribly wrong. PCI cares about forensics when things go wrong, i.e. what was stolen?, You care about the lesson learned so that it doesn't happen again. All security is about base-lining / white-listing / known-goods, and there is NO room for big data here. Determine what your systems SHOULD look like on a day to day basis, and report any variations. You will also need to report against: 1. Thresholds – you don't care if an admin fails to log in, you DO care if the same admin fails to log in 5 times in 3 seconds. 2. Critical events – every system / application / database has some

Req.	PCI DSS Update	Purpose / Need Addressed	Froud’s Comments
			events you should NEVER see, find out what they are and alert on them. 3. Trends – If you have only ever seen 1MB of logs come out of a system and suddenly you see 2MB, or none, alert on that too. Logging and monitoring is one of the most critical aspects of your security programme, and done correctly is one of the first lines of defence against the bad guys. Don’t do PCI minimums on this one.