The Definitive Guide to PCI DSS Version 4

Documentation, Compliance, and Management

—

Arthur B. Cooper Jr., Sec+, CISSP, CISA, CDPSE, CEH, QSA, PCIP
Jeff Hall, CISA, CISM, CDPSE, PCI QSA
David Mundhenk, CISSP, CISA, PCI QSA, PCIP
Ben Rothke, CISSP, CISM, CISA

Foreword by Bob Russo, Former General Manager, PCI Security Standards Council

Apress®

The Definitive Guide to PCI DSS Version 4

Documentation, Compliance, and Management

Arthur B. Cooper Jr.
Jeff Hall
David Mundhenk
Ben Rothke

Foreword by Bob Russo, Former General Manager, PCI Security Standards Council

Apress®

The Definitive Guide to PCI DSS Version 4: Documentation, Compliance, and Management

Arthur B. Cooper Jr.
Colorado Springs, CO, USA

David Mundhenk
Austin, TX, USA

Jeff Hall
Minneapolis, MN, USA

Ben Rothke
Clifton, NJ, USA

ISBN-13 (pbk): 978-1-4842-9287-7
ISBN-13 (electronic): 978-1-4842-9288-4
https://doi.org/10.1007/978-1-4842-9288-4

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: James Markham
Coordinating Editor: Jessica Vakili

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on the Github repository: https://github.com/Apress/The-Definitive-Guide-to-PCI-DSS-Version-4. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Authors

Arthur B. Cooper Jr. ("Coop") is a Principal Security Consultant at TrustedSec. He has 45 years of experience in information technology with the last 20 years focused on the security of payment systems and architectures, ecommerce, payment application assessments, forensic investigations, compliance security assessments, development of secure network architectures, risk management programs, security governance initiatives, and regulatory compliance. Coop was a member of the US Air Force (USAF) for most of his young adult life and had direct experience with the original ARPANET and ARPANET 1822 protocols. He was directly involved with the original DoD X.25 networks, the Defense Data Network (DDN), and the Automatic Digital Information Network (AUTODIN). He was directly involved with the original BBN Packet Switch Node (PSN) systems and has witnessed every major information technology "leap" or development since that time.

Coop was the standards trainer for the Payment Card Industry Security Standards Council (PCI SSC) for three years from 2010 to 2013 and has been a consultant to some of the largest retail companies and financial institutions in the world. He has worked with businesses to improve their overall security posture and to meet compliance regulations such as PCI, HIPAA, GLBA, and SOX. Coop is an experienced team leader and IT security expert who can ensure timely and successful completion of projects, as well as an enthusiastic security engineer researching emerging security technologies, trends, and tools. His certifications include Security+, CEH, CISA, CDPSE, CISSP, PCIP, and PCI QSA.

Jeff Hall is Principal Security Consultant at Truvantis, Inc. He has over 30 years of technology and compliance project experience. Jeff has done a significant amount of work with financial institutions and the healthcare, manufacturing, and distribution industries, including security assessments, strategic technology planning, and application implementation. He is part of the PCI Dream Team (DT) and is the writer of the PCI Guru blog, the definitive source for PCI DSS information.

David Mundhenk is Principal Security Consultant at the eDelta Consulting, as an information security, governance, risk, and compliance consultant with extensive multi-organizational experience providing a myriad of professional security services to business and government entities worldwide. He has worked as a computer and network system security professional for more than 30 years. David's experience covers a broad spectrum of security disciplines, including security compliance assessments, security product quality assurance, vulnerability scanning, penetration testing, application security assessments, network and host intrusion detection/prevention, disaster and recovery planning, protocol analysis, formal security training instruction, and social engineering. He has successfully completed 200+ PCI DSS assessments and scores of PA-DSS assessments. Certifications include CISSP, CISA, QSA, PCIP.

Ben Rothke, CISSP, CISM, CISA, is a New York City–based senior information security manager with Tapad and has over 20 years of industry experience in information system security and privacy. His areas of expertise are in risk management and mitigation, security and privacy regulatory issues, design and implementation of system security, encryption, cryptography, and security policy development. Ben is the author of the book *Computer Security: 20 Things Every Employee Should Know* and writes security and privacy book reviews for the RSA Conference blog and Security Management. He is a frequent speaker at industry conferences, such as RSA and MISTI, is a member of ASIS and InfraGard, and holds many security certifications, besides being an ISO 27001 lead auditor.

About the Technical Reviewer

Jeffrey Man is a respected information security advocate, advisor, evangelist, international speaker, keynoter, former host of "Security & Compliance Weekly," cohost on "Paul's Security Weekly," and Tribe of Hackers (TOH) contributor, including TOH Red Team, TOH Security Leaders, and TOH Blue Team, and he is currently serving in a consulting/advisory role for Online Business Systems. He has over 40 years of experience working in all aspects of computer, network, and information security, including cryptography, risk management, vulnerability analysis, compliance assessment, forensic analysis, and penetration testing. He is a Certified NSA Cryptanalyst. He previously held security research, management, and product development roles with the National Security Agency (NSA), the DoD, and private-sector enterprises and was a founding member of the first penetration testing "red team" at NSA. For the past 27 years, he has been a pen tester, security architect, consultant, Qualified Security Assessor (QSA), and PCI SME, providing consulting and advisory services to many of the nation's best known companies.

Author Introductions

Arthur B. Cooper Jr. ("Coop")

First of all, let me thank Ben Rothke. It was Ben who actually pulled together four ragtag old farts to assemble what would become known as the PCI Dream Team: Ben, Jeff, Dave, and myself. Together we have participated in many town hall–based webinars called "PCI Dream Team: Ask Us Your Toughest Questions," many of which were captured for posterity by BrightTalk.

Ben has also been very patient with me, as I am probably THE greatest procrastinator on writing anything for this book. This is not due to me not caring. In fact, quite the opposite. I care greatly about payment card security, and I have devoted the past 20 years of my life to the cause.

If anyone had ever predicted this is where I'd end up, I would have laughed and rebuffed them immediately. At the tender age of 17, I convinced my mother to sign some documentation allowing me to become a member of the US Air Force (USAF). No need to go into it all, but suffice it to say payments and payment security didn't rank high on my list of reasons to join up. However, the idea of security as a "calling" came to me at that very tender age of 17 when I saw what we (the USAF) were trying to accomplish. Security of my country rang loud in my ears, and I was hooked, pole, line, and sinker.

Some injuries, a "capture" of sorts, and some other maladies forced my hand, and I found myself being trained to work in military telecommunication centers. I didn't want to do that; I wanted to be some kind of superhero. Alas, my fortunes aimed elsewhere. At first, it didn't seem too exciting to me working in a closed building with no windows, and

I questioned my purpose and contributions greatly. Thank God I had some great military supervisors over the years, for they led me to the "promised land" of maturity and wisdom.

Let's flash forward many years and several ladder steps in my career. Around late 2004, I heard about the PCI standards being created. I jumped into the PCI arena with both feet and my eyes wide open. I was also fortunate enough to work for the PCI Council for a few years as a trainer, and all of my time on this journey has been very enjoyable. Hopefully I have been of some help to all of my clients over the years. I still love being a PCI QSA, and I always try to do the best I can when ensuring a client's compliance validation is accurate and timely and keeps them out of the news. I have been very fortunate, as NONE of my clients have ever been breached when I was working with them, and I'd like to think I had a small part in that.

I have no plans of ever retiring, unless it becomes medically impossible for me to help folks with their compliance and security needs. I work for the best cybersecurity firm on earth, and I will remain here until they pry my hands from the keyboard.

It has always been my honor and privilege to work with Ben, Jeff, and Dave on the PCI Dream Team and also with the entire PCI community for all these years.

Jeff Hall

The Guru and PCI

I started into the world of Payment Card Industry (PCI) compliance before PCI was even an acronym. In Fall 2002, I was running the information security practice at what is now RSM US and got a call from a partner to handle an engagement called a Visa security review – what turned out to be a Visa Cardholder Information Security Program (CISP) for one of the largest ecommerce retailers at the time, Circuit City.

My experience with security, as my experience with compliance, has followed a long and surreptitious route. I had flirted with both off and on throughout my career – first at KPMG, where I worked on occasional SAS 70 audits and did the odd mainframe security assessment, to finally coming fully into information security at RSM US.

From that first Visa CISP assessment, there was a lull for about a year, and then CISP assessments were becoming more and more common. I had been replaced as the head of the information security practice and moved into developing this new CISP service.

In January 2006, I was sent out to Foster City, California, to attend Visa's Qualified Data Security Professional (QDSP) training and obtain that certification as Visa was now requiring that to continue conducting CISP assessments. It was shortly thereafter that the PCI Security Standards Council was formed, and everything from the Visa CISP to Mastercard's Site Data Protection (SDP) program was transferred to the Council and became the PCI DSS version 1 and the Approved Scanning Vendor (ASV) scanning program.

As I did more and more PCI engagements, I had a lot of clients tell me I should write a book on the subject as they would tell me I had answers that they could not get anywhere else. While writing a book sounded intriguing, I thought the new form of publishing called "blogging" was an easier way to write, and so I created the PCI Guru blog in February 2009.[1] Since then, for better or worse, people have called me the PCI Guru.

At that time, there were plenty of topics to be discussed. My idea was to write something at least once a week, and I was easily able to make that happen. I also caught a lot of heat calling it the PCI Guru blog. After all, who was I to think that I was a guru of anything, let alone PCI? But as I have found out over all these years, there is still no source of PCI information quite like my blog.

[1] https://pciguru.blog

That leads to the importance of this book. There have been numerous books written about PCI over the decade and a half that the PCI DSS has existed. What makes this book unique is that it is written by QSAs that have more than a decade each of experience in the subject matter.

We have encountered all sorts of issues in those years that had to be resolved, from a vendor that deleted their customers' vulnerability scans in a software update to a client that had their SIEM fail and lost all their log data, to an equipment vendor managing a client's network that turned out to be unsegmented when they claimed it was segmented.

Yes, we have the audacity to call ourselves the PCI Dream Team, but that is exactly what we are. We are QSAs that are possibly some of the best if not the best QSAs around. Are we perfect? Oh, certainly not, and every one of us would admit that we have all made mistakes in our years of conducting PCI assessments.

But we have also solved some of the messiest and most complicated problems PCI has thrown at QSAs. It is not unusual for other QSAs to reach out to each of us personally or through our email account looking for advice as they encounter something they have never seen before.

From that, we have shared our experiences so that the PCI community can learn from our mistakes and successes so that the community is not continuously reinventing the wheel. This book is a continuation of that service to the PCI community by providing guidance for PCI DSS version 4.

David Mundhenk

Historically speaking, a measurably significant number of data breaches have been caused by flaws in applications and by the hackers who attempted to exploit them. In addition, hackers and threat actors have repeatedly targeted payment applications including ecommerce sites and point-of-sale (POS) systems. They do so because that's where the money is. Payment card applications have been specifically targeted and attacked

for more than two decades. This is why the major card brands have, and do still maintain, their own payment card security programs, in addition to supporting the PCI SSC and the PCI Data Security Standard (DSS).

I have worked in the payment card security space for more than 20 years now. I began working with payment card security first as an operational security engineer for the state of Texas, helping to ensure security and PCI DSS compliance of their state ecommerce portal and cardholder data environment (CDE).

Later, I moved on to work with IBM Security Services for seven years, first getting myself certified as a Visa Cardholder Information Security Program (CISP) assessor and then later as a PCI Qualified Security Assessor (QSA) and Payment Application QSA. Eventually I was selected to head up the IBM PA-QSA practice, which I led for six years.

From 2008 to 2010 and while still working for IBM, I was the sole QSA and PA-QSA for the world's largest payment processor. I traveled the globe at their request to help them assess their many different payment processing environments and applications.

I also helped them test and certify almost a dozen PA-DSS qualified applications from point-of-sale (POS) systems and ecommerce applications running on mid-range systems all the way up through tier 1 payment card switches that connected directly to the major payment card networks. It was almost like going to graduate school in payment card security.

I eventually left IBM to join Coalfire's Application Security team where I worked to test and certify all manner of application architectures, but with a special focus on PCI applications. It was there that I also got P2PE QSA and P2PE PA-QSA certified.

After leaving Coalfire I moved on to the Herjavec Group (HG) as a GRC team lead working on all things GRC but especially PCI DSS work. As of the writing of this book, I am currently working as the PCI practice lead for eDelta based in NYC.

I have also been publishing and copublishing online articles and papers related to cyber- and PCI security since 2007, many of which have

been co-authored with my good friend and co-author of this book Ben Rothke. It was Ben who actually pulled together what would become known as the PCI Dream Team: Ben, Jeff, Coop, and myself. Together we have participated in many town hall–based webinars called "PCI Dream Team: Ask Us Your Toughest Questions," many of which were captured for posterity by BrightTalk.

I truly believe that payment card security has done more to raise cybersecurity awareness for the general public than any other cybersecurity standard I have worked with. After all, the majority of the public use payment cards in one form or another.

Many of us have gotten that dreaded letter from our banking institution informing us that our payment card account has been compromised. So most people fully understand how important this subject is because most of them use payment cards in one form or another.

One of my favorite sayings is "…a rising tide floats all boats." I often close our webinars with the premise that the PCI Dream Team is not four crusty old farts espousing the virtue of payment card security. The PCI Dream Team is really a "community" of folks including all of you who understand how important this subject is and do their part as well to help ensure payment card security is paramount and maintained at the highest levels of quality possible.

It has been my honor and privilege to work with Ben, Jeff, Coop, and all of you while we work together to help raise the tide of awareness for all.

Ben Rothke

My PCI Journey

In 2016, I was a senior security consultant with Nettitude, an information security consultancy. I had been a Qualified Security Assessor (QSA) for a few years and found that even as detailed and prescriptive as the PCI Data Security Standard (DSS) was, my clients still had many PCI questions.

I found that, too often, these clients would direct their PCI questions to their hardware or software vendors expecting an unbiased answer. As often is the case with vendors, they will push their own solutions, rather than look out for the customers' best interests.

Sometimes these clients would ask their security consultants or advisors – who, while having extensive information security experience, were not QSAs or lacked expertise in the payment space – for advice, and their suggestions would often not be in line with what the PCI DSS required. At the same time, their suggested answers were acceptable from an overall security perspective. By not answering relevant to the PCI DSS, these answers put clients in a PCI non-compliant state.

With such issues in mind, I thought it would be a good idea to get some experienced security PCI professionals together and answer PCI questions. We would do this unbiasedly, not pushing products or services of the firms we were working for.

I reached out to three of the smartest PCI professionals I knew and suggested we do a webinar, which was the start of the PCI Dream Team. The first iteration[2] of the PCI Dream Team consisted of authors David (whom I worked with previously on a PCI project for a large entertainment company) and Coop (who led my QSA training and, in my experience, is one of the best technical trainers ever), in addition to my Nettitude colleague at the time, Jim Seaman.

In 2017, the next and current iteration[3] of the PCI Dream Team bid adieu to Jim and welcomed author Jeff to the team, and we've been a band of PCI brothers since. Many people know Jeff via his PCI Guru blog.[4] It's not just the name of his blog; Jeff *really* is a PCI guru.

So why is this book necessary? There are several existing books about PCI in print, from *PCI DSS: An Integrated Data Security Standard Guide*

[2] www.brighttalk.com/webcast/288/207869

[3] www.brighttalk.com/webcast/288/245165

[4] https://pciguru.wordpress.com/

(Apress) by former Dream Team member Jim Seaman to *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance* (Syngress) by Branden Williams and Anton Chuvakin, the upcoming book by Branden *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance*, and more.

What is unique about this book is twofold. Here, we tell you exactly what you need to provide your QSA for *every* PCI requirement. Even though the PCI DSS is quite prescriptive (much more so than standards and regulations such as ISO 27001, HIPAA, GLBA, SOC 2, GDPR, and others), a merchant or service provider can often be left scratching their head not knowing precisely what they need to show their QSA during an audit.

Here, we detail what specific documents we, as QSAs, need to see to attest to your PCI compliance. No other reference has this documentation list the particular documentation requirements for every one of the over 400 requirements of PCI DSS version 4.

The second benefit of the book is that we bring real-world experience and unbiased advice to every page of the book. We are keeping theory to a minimum and focusing on the real-world scenarios that most merchants and service providers face in their quest to achieve and maintain PCI compliance.

We are not reinventing the wheel here, so we won't be sharing information that has already been printed, the objectives of PCI DSS compliance, or other information easily available on the PCI website. We could have easily made this into a 1,000-page reference, which would gather dust. But we'd rather have it be leaner and of value. Our book is meant for PCI practitioners, so we expect the readers to have a decent understanding of payment systems, the PCI DSS itself, and other things fundamental to PCI.

The authors have more than 50 years of combined PCI experience and 100 years of information security and risk management experience.

We have seen it all, been there, and done that. And we are sharing our combined knowledge with you, to make your PCI journey easier.

We hope you enjoy reading this book as much as we enjoyed writing it. In case we didn't answer your question here, feel free to email us at pcidreamteam@gmail.com.

Foreword

My father always told me that if you stick around long enough, you get to see some pretty amazing things. In the case of credit card security, he was 1,000% right. I was lucky enough to be in the data and network security business most of my career and even luckier to be loosely associated with the major credit card companies in that capacity early on. I was fortunate to play a very small part in the early days and proliferation of the PCI Security Standards Council and the promotion of most of the standards they created.

The authors of this book, Jeff, Coop, Dave, and Ben, on the PCI DSS have also collectively been associated with the security business, specifically these standards, for over 50 years. Like my dad said, you see some pretty amazing things if you stick around long enough and, more importantly, if you're paying attention!

The authors have been in the thick of it right from the beginning and have obviously been paying very close attention. They have seen the industry go from what a security expert might refer to as the wild wild west to one that has become the poster child for the saying that you "must bake security in from the beginning" on everything it does.

They not only know this standard and all of its iterations, but throughout the years, they have worked with it closely and helped vast amounts of companies secure their customers' credit card and personal data. They have been involved in the review of these standards and the implementation of them in every scenario you could possibly imagine.

They have watched how credit card data security has evolved and worked with the PCI DSS from its first version and through all of its iterations up to today's version 4.

The PCI SSC DSS was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. It provides a baseline of technical and operational requirements designed to protect payment account data.

The updated PCI DSS v4.0, released in March 2022, continues that mission by ensuring the DSS continues to meet the security needs of the payments industry, adds flexibility to support different methodologies used to achieve security, and enhances validation methods and procedures. Security needs to be a continuous process, and adherence to the PCI DSS v4.0 helps make that possible.

So whether you're a merchant trying to protect your customers' credit card and personal data or a security person responsible for implementing and maintaining the PCI DSS in your organization, this book will help you understand and have the best possible chance of keeping your precious information safe and secure.

And to quote *Hill Street Blues* (look it up): Let's be safe out there, people.

Bob Russo
Former General Manager, PCI Security Standards Council

CHAPTER 1

A Brief History of PCI

Welcome to the PCI DSS

Most people think that PCI began with the formation of the PCI Security Standards Council (PCI SSC) back in 2006, but the roots of PCI, in fact, go back to the late 1990s.

With the advent of the Internet and the development of electronic commerce, the card brands (American Express, Discover, JCB, Mastercard, and Visa International) began to see breaches of cardholder data (CHD) from the very beginning. The first brand to enter the security domain was Visa, with the creation of its Cardholder Information Security Program (CISP) around 1999.

In those days, the CISP was just a set of glorified Excel spreadsheets with the security requirements defined along with their testing. One of the authors (Hall) did one of the first independent CISP assessments in 2002–2003 for the now defunct retailer Circuit City.

However, all that was examined at that time was their ecommerce operation, not their physical stores. A funny thing about that first assessment was that the Excel spreadsheet was full of comments explaining who the actual developer of that program was – Deloitte.

Not to be outdone, Mastercard came up with their Site Data Protection (SDP) program around 2001 or 2002. Its notable contribution to security was the periodic vulnerability scanning of online ecommerce assets and

A. B. Cooper Jr. et al., *The Definitive Guide to PCI DSS Version 4*,
https://doi.org/10.1007/978-1-4842-9288-4_1

the Approved Scanning Vendor (ASV) concept. American Express followed with their Data Security Operating Policy (DSOP), Discover entered the fray with the Discover Information Security and Compliance (DISC) program, and JCB came up with their Data Security Program.

As you can expect, retailers were not excited to have anywhere from three to five security programs to comply with by January 2004, and they were loudly clamoring for a solution. The problem was that the legal departments at the card brands viewed any consolidation of their security programs as a violation of antitrust and collusion laws in the United States. Regardless, everyone involved agreed that a solution needed to be found. The situation was further exacerbated in Spring 2004 when Visa decided to push their CISP into the brick-and-mortar realm as they started to see breaches move from the Internet into physical retail store environments.

Between 2004 and 2006, several changes were seen. To alleviate retailers' compliance heartburn, American Express decided in mid-2004 to accept a Visa CISP assessment for proof of compliance with their DSOP. That was followed by Mastercard and Discover in early 2005, acknowledging acceptance of a CISP report instead of their own, although Mastercard kept their online security program of vulnerability scanning in place.

At the beginning of 2006, Visa began its Qualified Data Security Professional (QDSP) certification program to address the inconsistencies in CISP assessments that were now performed mainly by consultants. Three sessions were held between January and April 2006 at Visa's headquarters in Foster City, California. It is worth noting that three of the authors (Cooper, Hall, and Mundhenk) are all holders of the rare QDSP certification.

Finally, in early 2006, the legal powers that be at the card brands came up with the concept of the PCI Security Standards Council (PCI SSC), or the Council. With the formation of the Council, the Visa CISP (now branded the PCI DSS v1.0) was adopted as the PCI DSS v1.1 with some minor changes.

Mastercard's SDP online assessment program became v1.0 of the Approved Scanning Vendor (ASV) program. QDSPs were grandfathered into the program as the first QSAs, with formal QSA training starting in 2007. And with that, the PCI DSS process was born. The final piece of the puzzle was the first PCI Community Meeting held in Toronto, Canada, in October 2007 for all QSAs and ASVs.

How We Got to Today's PCI DSS

The PCI DSS v1.0 was actually published by Visa for their QDSP training. It was PCI DSS v1.1 that was published by the PCI Council in September 2006. This version adopted the PCI SSC's logo and contained some updated language and testing from v1.0 that focused on the standard being under new ownership.

In October 2008, the Council issued v1.2 of the PCI DSS. One of the biggest changes in this release was the adoption of the term "assessment" vs. "audit" due to CPAs arguing that under state laws, only CPA firms could conduct an "audit." Other changes focused on increasing the scope of the assessment from an external perspective to a 360-degree look at the payment environment and anyone that had access to the cardholder data environment (CDE). The other major change was the reordering and renumbering of requirements, which caused issues for many QSAs.

July 2009 brought us v1.2.1, which was mostly editorial corrections but did provide for the first time an example of a filled-out compensating control worksheet, something that was desperately needed.

October 2010 gave us the first major revision of the PCI DSS. v2.0 of the DSS brought us separate documents for the Report on Compliance (ROC) and the Attestation of Compliance (AOC). This version also began the alignment of the DSS with other PCI standards that had been published such as the PIN Transaction Security (PTS) standard and the Payment Application Data Security Standard (PA-DSS). The version also

brought a number of clarifications that explicitly called out technologies such as virtualization to ensure that all elements of the cardholder data environment were assessed. Also around this time, the PCI Council announced that they would begin publishing standards updates on a three-year schedule.

The publication of v2.0 of the PCI DSS also brought the start of the Assessor Quality Management (AQM) process. Up to this point, QSACs had been filling out Reports on Compliance and Self-Assessment Questionnaires with no guidance as to what the Council and card brands expected. As it occurs today, QSACs were required to turn over a sample of their v1.2.1 assessments to the Council for AQM review. What QSACs found unfair about the rollout of the process was that they were given the AQM assessment criteria after the fact. It was like taking a test on a subject matter you had never been given. The result was that almost every QSAC was placed into remediation over the next year. Worse, other QSACs took advantage of those in remediation and told prospective clients that QSACs in remediation could not perform their PCI assessments, which was not true. The Council took a lot of heat from QSACs for the first AQM assessments. The Council also had to repeatedly tell QSACs and the public that QSACs in remediation were still allowed to perform assessments. It was not a good time for the Council or the PCI DSS program.

Following their three-year standards update schedule, the Council issued v3.0 of the PCI DSS in August 2013. This update to the DSS was coordinated with the update to the PA-DSS. The biggest change with v3.0 was its focus on addressing the threats that organizations had encountered in the preceding three years. Another focus of this update was to even further clarify and explain what was expected of QSAs in assessing entities for PCI DSS compliance as the AQM program was still finding significant inconsistencies in assessments. Key areas identified by the Council for the changes in v3.0 were identified as