Verizon 2016
Payment Security Report

Insight for helping businesses manage risk through payment security.

verizon✓

Verizon 2016
Payment Security Report

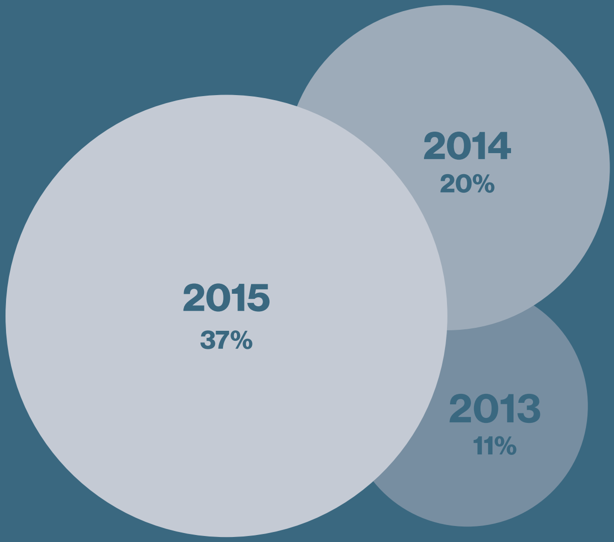
Part 1

Part 2

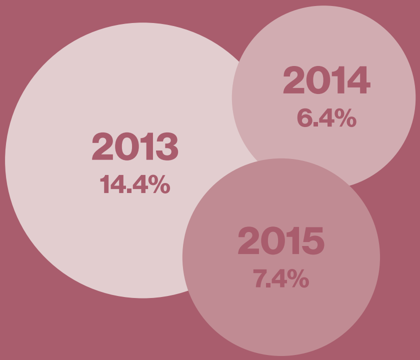
Appendices

The good news is that compliance is still going up, but it's not quite that simple...

Full compliance



Average control gap



Introduction

Good news, and bad

The good news is that compliance is still going up. In 2015, 37.1% of Verizon's PCI DSS assessed companies were fully compliant at interim validation compared to 20.0% and 11.1% in previous years. But that still means that nearly two-thirds of companies are failing to maintain compliance from year to year.

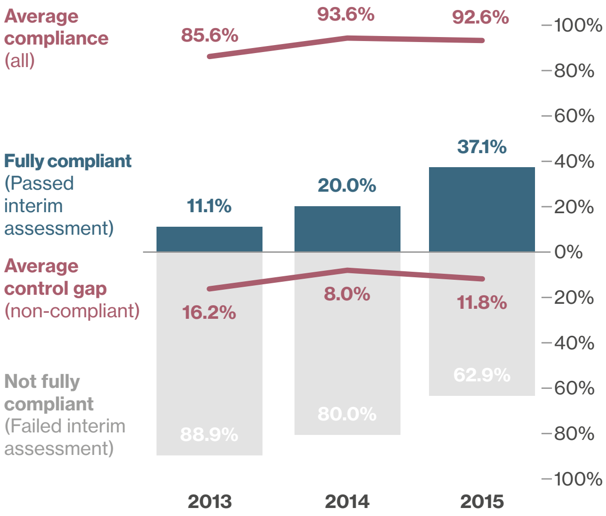


FIG 1 – Change in average and full compliance, 2013 – 2015

While the number of organizations maintaining compliance has increased, those that did not achieve 100% compliance showed a slight widening of average control gap – the percentage of controls failed. In 2014 organizations failing their interim assessment had an average of 8.0% controls not in place (6.4% across all companies). In 2015 this went up to 11.8% (7.4%).

These aren't just a few niggling rules. Many of the controls that were not in place are quite important and could be material to the likelihood of suffering a data breach.

This report strives to reveal where companies are falling short and exposing themselves to business risk. It will help you to understand:

- What must we start doing?
- What must we stop doing?
- What must we do more of?

Other payment security resources

We've created a range of resources to help you get the most from our research. Our executive summary brings you the key findings and messages in just a five-minute read. And our infographic reveals the top three security challenges by industry. Share these resources with your colleagues to educate them on the importance of payment security. Find out more by visiting:

VerizonEnterprise.com/PaymentSecurityReport

Section 1:
Executive summary

This report is the only major industry publication that is based on data from real compliance assessments, conducted worldwide. Insights from our post-data breach investigations make it a unique resource.

It has been ten years since the Payment Card Industry Security Standards Council (PCI SSC) released the Payment Card Industry Data Security Standard (PCI DSS) version 1.1, and six years since the publication of our first PCI report. Large-scale data breach disclosures are increasingly common, with millions of sensitive records compromised each year. Many organizations, including the US government, are discussing what can be done to protect customers and organizations against the onslaught of attacks.

Verizon has been on the frontline of cardholder data security since 2003. The Verizon Payment Security Report, now on its fifth edition, has become the go-to resource for industry experts because of its critical evaluations on the performance of the PCI DSS, its insights on the evolution of payment security, and debate on the ability of organizations to meet sustained compliance.

The state of compliance

PCI DSS specifies a minimum set of security controls to protect payment card data, but it doesn't explicitly specify how organizations should go about monitoring and evaluating the effectiveness of those controls once they are implemented.

In 2015, organizations in the IT services industry achieved the highest average compliance (98.1%), followed by retail and hospitality organizations (93.6%) and financial services providers (90.4%).

As in previous years, organizations in every industry continue to struggle with security testing, especially in the area of network vulnerability assessments.

But there's some good news. Several controls, including 11.2 (Run network vulnerability scans) and 11.3 (Implementation of penetration testing), showed year-over-year improvement, with full compliance for Key Requirement 11 (Test security systems and processes) increasing 36.7 percentage points between 2014 and 2015, and reaching 70.0%.

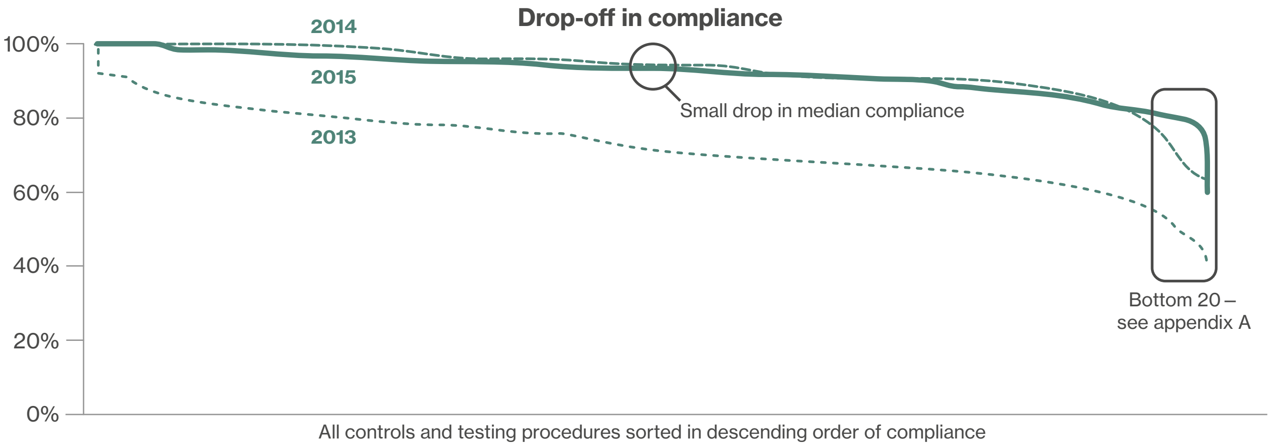


FIG 2 – Drop-off in compliance: comparing 2013, 2014 and 2015

> Once system complexity gets to a certain level, mistakes are almost inevitable—but still predictable.

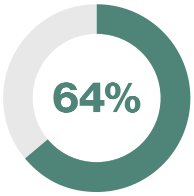
Control effectiveness

This year's report provides further insights about the payment security control failures that lead to breaches, and how to prevent them. This year we address the crucial topic of "control effectiveness". This is an issue that is often raised in the context of payment card data protection, but which seldom receives an adequate response.

> Control effectiveness: the degree to which the design and operation of a security control is successful in achieving the intended risk mitigation.

When it comes to control effectiveness, we took a familiar approach with in-depth worldwide evaluation of PCI Data Security regulation compliance. We probed performance against the PCI DSS 3.1 standard, to understand specific challenges within each geographic region and industry vertical. This involved deep dives into each of the DSS Key Requirements and associated base controls, right up to the individual testing procedures.

Hang on to your hat, because we uncovered some surprising findings that could be critical to your practice of security effectiveness, potentially averting unnecessary breaches and saving millions in lost revenues – not to mention tarnished reputations.



of consumers are unlikely to do business with a brand that has suffered a data breach[1].

Types of assessment in this report

Interim validation

A compliance assessment carried out by a Qualified Security Assessor (QSA), or Internal Security Assessor (ISA), ahead of the annual validation. This can result in zero (a pass) or more non-compliances. The output is an interim Report on Compliance (iRoC).

Final validation

A formal annual compliance validation usually conducted once all previously identified non-compliances have been remediated within a defined time frame. The output is a final Report on Compliance (fRoC).

Post-breach investigation

An investigation conducted by a PCI Forensic investigator (PFI) following a suspected data breach.

Time taken for remediation

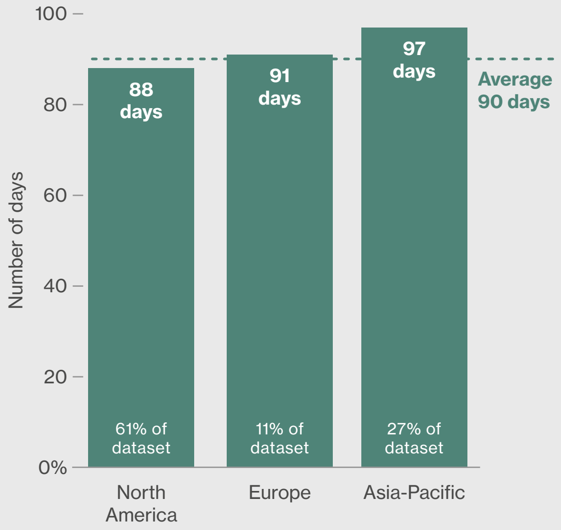


FIG 3 – Time taken for remediation (see page 55 for methodology)

Section 2:
Compliance effectiveness

Debating the effectiveness

How effective PCI Security standards are in protecting businesses and consumers against data compromises is an ongoing debate. This is especially true after the disclosure of data breaches involving the large-scale compromise of payment card data, where it is typical for organizations to claim that they did what they believed was required to protect sensitive data.

Between 2010 and 2015, Verizon's RISK (Research, Investigations, Solutions and Knowledge) Team found that only about 9% of organizations that experienced a confirmed payment-card-related data breach had initiated PCI DSS compliance programs and validated compliance prior to the event.

None of the organizations that experienced data breaches were maintaining all applicable PCI DSS controls at the time of the breach, according to the Verizon investigative team that analyzed the data that appeared in the Verizon Data Breach Investigations Report (DBIR)[2]. Not one organization could provide evidence that it had achieved sustainable compliance and maintained a set of resilient controls. All of the organizations failed to have multiple PCI DSS Key Requirements in place – including controls that were material to the breach.

Our experience suggests that organizations that are able to successfully maintain all applicable security controls:

- **Think about controls in the context of an effective control environment.**
- **Implement additional security controls over and above the minimum baseline set of controls.**

> “Our research shows that most organizations fall out of compliance within three to nine months of their last formal compliance validation.

Without an explicit need to test the resilience and effectiveness of their PCI DSS controls, many organizations are taking a “fire and forget” approach to control implementation. Control effectiveness is not a primary concern in their standard compliance operations and data protection programs.

Hence, some organizations question whether the PCI DSS is adequate to protect cardholder data. It's not just the controls in the PCI DSS themselves, but the approach taken to implement them, that determines their effectiveness. Perhaps this needs a more explicit clarification in future versions of the standard – particularly since many organizations do not have the skills to problem-solve that on their own.

> “The likelihood of control failure (control risk) can be determined by frequently monitoring the inherent risk x residual risk x detection risk of each control.

Security can only be achieved through ongoing monitoring of well-designed controls to verify they are operating effectively at all times, and modifying them if they are not. The most successful organizations rely on intelligent control systems that are actively measuring and managing the effectiveness of implemented controls. These organizations continue to add controls (beyond the PCI DSS) to achieve a resilient and sustainable control environment that can also address future risk.

With the release of PCI DSS version 3.2 in April 2016, it was declared to have reached maturity[3]. However, this version didn't include explicit recommendations for how organizations should achieve control effectiveness. Since PCI DSS 3.0, the standard has included a section "Best Practices for Implementing PCI DSS into Business-as-Usual Processes" with recommendations for monitoring the effectiveness of security controls and the cause of control failure.

A slow evolution

In November 2012, the PCI SSC released the "Information Supplement: PCI DSS Risk Assessment Guidelines" that provides guidance for executing risk assessments. While this was a good start, and included cursory recommendations on residual risks and control effectiveness, it did not explicitly cover control risk.

> Over the last three years, the DSS has been updated more frequently than ever before.

The PCI SSC began to apply more focus on compliance sustainability, initiating a "make PCI DSS part of business as usual" campaign. In August 2014, the PCI SSC released an "Information Supplement: Best Practices for Maintaining PCI DSS Compliance". It provides best practices for maintaining compliance with PCI DSS, after an organization has already undergone an initial PCI DSS assessment and successfully achieved compliance. It includes detailed recommendations on a range of measures that can be used to monitor whether program-level and system-level security controls are implemented correctly, operating as intended, and meeting the desired outcome[4].

Early PCI DSS versions did not define an integrated "risk-based approach" for control evaluation – at least in part because there is a lack of consistency in the application of risk management across the industry.

> A discussion about control systems is critical to the future evolution of the PCI DSS and giving the standard even more credibility among security practitioners. That's why we're spotlighting control effectiveness.

The PCI SSC published the "Designated Entities Supplemental Validation" (DESV) in June 2015, and later included it in PCI DSS 3.2 as Appendix A3. It includes requirements specifically intended to monitor effectiveness of security controls and minimize risk of control failure; e.g. Requirement A3.3 Validate PCI DSS is incorporated into business-as-usual (BAU) activities. PCI DSS 3.2 also includes requirements for service providers based on DESV, including control 10.8 (Implement a process for the timely detection and reporting of failures of critical security control systems).

Considering the global reach of the standard across various industries, and the range of businesses to which it applies – from small to very large – introducing an organization-led risk-based approach would be a challenge. It would need to be carefully managed to avoid being susceptible to the following failings:

- Many organizations wouldn't know how to objectively perform risk management; it may require skills beyond their capabilities.
- Organizations may fail to define an appropriate risk level (the amount of risk they find acceptable) or have too high a risk tolerance (the maximum amount of risk they accept), or may be inconsistent with how they apply their acceptable risk level to risk decisions.
- Organizations might decide, based on their risk assessment (which often is more perception than actual measurements), that some PCI DSS controls are not needed.

Industry awareness that risk management is integral to data protection and compliance has increased. While other international standards provide firm guidance on suitable risk management methodologies, the PCI DSS does not explicitly integrate such a requirement into the standard. The PCI DSS would benefit from introducing stronger requirements for the deployment and operation of controls, to include the need to actively measure control effectiveness, constraints and efficiency. At present, the evaluation of control risk is only partially addressed within the compensating control worksheets. PCI DSS controls (and additional controls) must be implemented, regardless of any perceived lack of risk.

> Control effectiveness must be objectively measured throughout the control lifecycle.

Control failures and data breaches

The PCI DSS was first released in December 2004[i]. Between then and 2014, the number of large-scale data breaches grew significantly. This led many, including the media, to ask why compliant organizations were still being breached.

Data should always be protected by layers of security. Breaches occur due to absence or failure of one or multiple security controls. Controls fail due to weaknesses in design, operation or maintenance that make them ineffective. This is, in many cases, the result of an ineffective control environment.

The answer lies in the failure to understand the nature of control effectiveness and a tendency to underestimate the importance of control resilience across industry verticals – which we exposed in the 2014 and 2015 Verizon PCI Compliance reports.

> Controls should address measured risk by design, and should not be implemented merely to meet compliance requirements.

For any PCI DSS "compliant" organization that has suffered a payment card breach, specific controls must have failed for the security perimeter to be breached and, in addition, other controls must have failed thus allowing data to be compromised[ii].

When a breach occurs, organizations often focus on investigating the failure of entry-point controls. They rarely dig into underlying failures in risk management, control lifecycle and effective control management – and if they do, they rarely share their findings.

Practitioners would benefit from additional guidance on how to assess control effectiveness and implement intelligent control management.

Any framework to assess control effectiveness must be dynamic. It must explain control concepts, methods for defining controls, control lifecycles, control systems and control environments. It must require risk-to-control mapping, and deliberate cause-and-effect evaluation as part of a control lifecycle process.

> Organizations that make sustainability and resilience part of their compliance operating procedure have a significant head start over those that focus solely on achieving DSS compliance.

Control concepts

Security controls can be classified into one of the following four categories:

- **Preventative controls** deter problems before they arise – e.g. physical controls and passwords.
- **Detective controls** discover problems when they happen – e.g. log reviews, inventories, penetration tests and vulnerability scans.
- **Corrective controls** resolve problems after they arise and return the system to a "normal" state.
- **Directive controls** are actions taken to cause or encourage desirable events to occur – e.g. policies and training.

[i] The very first version of PCI DSS, version 1.0, was released by Visa US in December 2004.

[ii] Not all control failures result in data breaches. Data breaches can happen either because controls aren't in place (missing) or because the controls weren't used or maintained. Sometimes other controls may prevent unauthorized disclosure; or you might just be lucky.

What does an effective control system look like?

For a control system to be effective, controls must be resource-efficient and budget-friendly, and should be reviewed periodically. They should also be able to react to changing business priorities and threats.

In a PCI DSS context, this requires procedures to promote understanding of risk exposure, putting controls in place to address those risks, and effectively pursuing the cardholder data protection objectives, which include effective and efficient processes, reliable data protection and compliance reporting, and compliance with policies, regulations and applicable laws.

Definitions

Control: The means by which the use of limited resources is directed, monitored and measured. It regulates organizational activities so that a targeted element of performance remains within acceptable limits, and to ensure that risks, which may inhibit the achievement of objectives, are kept to a minimum.

Control assessment: The systematic review of processes to check controls are still appropriate and effective.

Internal control: The procedures established to create business value and mitigate risk. A process designed to provide reasonable assurance of:

- Effectiveness and efficiency of operations.
- Reliability of reporting.
- Compliance with applicable laws and regulations.

Control correctness: A level of assurance that the security mechanisms of a requirement have been rightly implemented[5].

Control effectiveness: A level of assurance that the requirement of the system meets the stated security objectives[5].

Control environment: The actions, policies, values and management styles that influence and set the tone of the day-to-day activities of an organization; a reflection of the values of an organization; the atmosphere in which people conduct their activities and carry out their control responsibilities.

Control framework: A structure that organizes and categorizes an organization's internal controls to help it develop good internal control systems. A number of frameworks have been created, including:

- The COBIT framework.
- The COSO internal control framework.
- COSO's Enterprise Risk Management framework.

The security control lifecycle

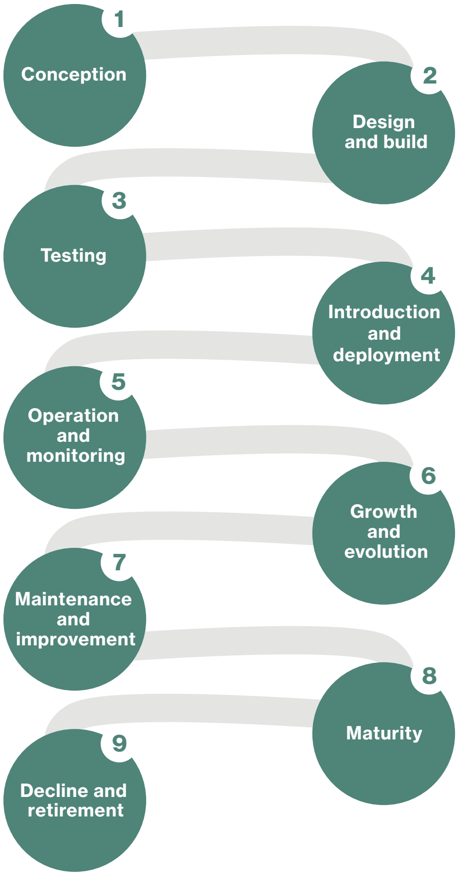


FIG 4 – Control lifecycle (see also Appendix B)

Control resilience: The ability of a control to resist and recover from unwanted change.

Control risk: The risk caused by controls losing effectiveness over time and exposing the assets they were intended to protect, or failing to prevent such exposure.

Control system: Management activity to maintain a collection of procedures designed to record, verify, supervise, authenticate, and, where necessary, restrict access to assets, resources, and systems.

Control is when the outcome can be predicted; when the actions you are taking can be expected to achieve a specific intended outcome that is predictable. The predictability of the outcome depends on the quality and timely input of data, information, knowledge and insight.

The data breach chain shows how breaches happen in five steps. Break the chain and prevent the breach.

The need for active control effectiveness monitoring

Data breaches occur because of a lack of control effectiveness and control resilience – even at organizations that have implemented PCI DSS and passed a compliance validation. The controls may have been implemented but were never effective, or they were not designed to be resilient enough to offer sustainable protection, despite changes in the environment.

> Security breaches and data compromises occur either because a control is missing (i.e. not in place; inactive/not operational), or the control was operating as designed, but was knowingly or unknowingly ineffective.

We see numerous examples of controls that are compliant (and therefore "correct") but not necessarily effective. For example:

- Traditional, signature-based anti-virus systems that fail to detect significant amounts of malware.
- Firewalls that are fully operational but only perform stateful inspection and are not configured to use their full application and context-aware filtering abilities, reducing their ability to prevent attacks.

To significantly reduce the chance of a data breach, organizations need to implement a monitoring process that measures the effectiveness of all PCI DSS controls against their objectives on an ongoing basis. This requires consistent measurement of both the performance of individual controls and their effectiveness within the context of the overall control environment to record and report the risk mitigation capability of each control. We cannot emphasize enough that, based on our extensive research, this process needs to be included as a compliance requirement in future iterations of the PCI DSS.

The data breach chain

Valuable data is stored

🔓 **Valuable payment account data is stored, processed, or transmitted to, from and within various networked system environments.**

🔒 Consider the use of tokenization or strong encryption (see P2PE on page 16).

Access is not managed effectively

🔓 **People, processes and technology within the data environments allow ingress and egress.**

🔒 Without any access to the data, or ability to retrieve it, the data cannot be compromised. Enhance authentication controls and isolation of environments and system components.

Control management is insufficient

🔓 **A collection of detective, preventative and corrective security controls are put in place to protect the data and to correct or mitigate weaknesses in the environment, but are not monitored and maintained.**

🔒 Controls only provide reasonable assurance. Increase frequency of control performance evaluation of all controls throughout the control lifecycle, including a comprehensive evaluation of the control environment.

Controls become ineffective

🔓 **Inherent or residual weaknesses in the design, implementation, or operation of controls can expose system components that allow direct or indirect access to the data.**

🔒 Increase the resilience of controls and the control environment – its ability to resist change and "bounce back" from unexpected changes.

Compromises aren't spotted fast enough

🔓 **Threat actors exploit vulnerabilities, resulting in a security breach and data exposure.**

🔒 Measure, report and act. Enhance data and security monitoring, detection and response competency through automation, training and performance measurement.

Implementation of PCI DSS requirements involves two interdependent aspects: effectiveness and correctness.

PCI DSS controls should be designed and implemented to mitigate risk to account data as well as risks to the supporting system components in, and connected to, the cardholder data environment (CDE). The PCI DSS is made up predominantly of preventative controls and a number of detective and directive controls. However, it's inevitable that the risk environment will change, and controls will eventually fail. The detective controls currently included in the PCI DSS, such as running vulnerability scans, can be strengthened with additional corrective controls and comprehensive mechanisms that can identify where corrective controls are required.

> Understanding the various key processes, stakeholders and relationships is important in the development of a successful and sustainable compliance program.

Control correctness and effectiveness

Independent compliance validations (which are different from security validations) follow a set of prescribed testing procedures conducted in a limited time. They offer a limited and non-exhaustive verification of security controls, mainly determining whether controls are "correctly" implemented.

Effective controls, however, need to meet a resilience standard when carrying out their intended functions. They need to withstand environmental changes in system operations as well as attacks. Thus, many controls may satisfy correctness criteria (compliance), but fail to meet effectiveness criteria (actual security), particularly under unanticipated conditions.

Control performance vs effectiveness

The performance of security controls should be measured to determine achievement against an established standard benchmark. For example, the required performance for both internal and external vulnerability scans is one clean scan per quarter as well as after any significant changes.

Effectiveness takes into account the probability that a control will be successful in meeting its intent and its rate of achievement. Its measurement is based on the amount of time a control meets its intent while in operation, and the amount of time it remains in operation without disruption. It assumes that past achievement is a good indicator of future success.

In addition, while conducting their own internal compliance validations, organizations will often deem controls to be effective merely by their presence but fail to determine whether they are performing as expected, and at all times. Ultimately, an evaluation of the correctness and effectiveness of a control should be done through direct measurement and reasoning, which will involve an assessment of control design, installation, operation and performance, as well as evaluation of residual risk and control risk.

An effective control environment is defined as "an environment in which competent people understand their responsibilities, the limits of their authority, and are knowledgeable, mindful and committed to doing what is right and doing it the right way. Employees in this environment are committed to following an organization's policies and procedures, and its ethical and behavioral standards."[6]

> During PCI DSS compliance assessments, we often see familiar weaknesses in the management control systems.

Control systems

Requirements for control lifecycle management and performance monitoring lack the attention we believe they deserve in PCI SSC program documentation. Several characteristics of "control systems" are recommended or strongly implied within the "Best Practices for Maintaining PCI DSS Compliance" information supplement, but the concept is not explicitly defined in the PCI DSS[4].

During PCI DSS compliance assessments, we often see familiar weaknesses, including:

- Lack of formalization of the management control system, i.e. not assigning resources with defined roles and responsibilities, and implementing and maintaining processes backed by supporting policies and procedures and technology (12.4).

- Lack of effective security awareness training or frequent communication to reinforce data protection and compliance goals (12.5, 12.6).

- Failure to verify that managers and employees understand their responsibilities and to provide the means and support they need to fulfill them (1.5, 2.5, 3.7 etc.).

- Control system designs that cannot adjust to changes in the business and/or data protection environment.

- The absence of mechanisms for measuring and reporting performance that cover all critical data protection and compliance performance metrics, leading to a failure to communicate the results of data protection and compliance actions across the organization.

Any of these behaviors weakens the control effectiveness of the compliance environment (cardholder data environment and connected systems) and increases the risk of data being compromised.

Data protection cannot be achieved solely by making small incremental improvements based on the PCI DSS, which is just a general-purpose set of baseline controls. Controls operate within a structure (framework) managed by a system of policies and procedures (a control system). A control system must be designed; it will not create itself. It has critical points (success factors), such as:

- **Acceptance:** Employee involvement in the design and maintenance of controls has been found to increase acceptance of and adherence[7].

- **Accuracy:** Metrics obtained from control systems must be accurate and should be useful, reliable, repeatable and consistent.

- **Comprehensibility:** Controls must be simple and easy to understand, operate and maintain.

- **Integration:** Controls must work in accordance with procedures without creating unnecessary effort, operational delays or bottlenecks.

The effectiveness with which security controls are managed at each step of their lifecycle (see Appendix B) determines the likelihood of control risk creating exposure and potential data breach.

Section 3

Payment security innovation

Mobile payments

The uptake of mobile as a payment device by both merchants and consumers has been steadily rising. As consumers we can choose to turn our phone into a payment token, so it operates just the same as a debit or credit card, and we can ping money to whomever we want using an email address or a telephone number.

From a payments perspective, mobile has the potential to revolutionize the way payments are authenticated. The capabilities of the devices themselves can be used to provide multi-factor authentication, including biometrics, soft-token-generating applications (like Google Authenticator), and token receipt via SMS. Further, meta data about the device (IMEI – International Mobile Equipment Identity) and the location (via geolocation) can also be harnessed to provide greater assurance that the transaction is legitimate. Other benefits that can be achieved through mobile payment technology include:

- Better device authentication (cards registered to devices use identifiers unique to each device).
- More variables for context-specific access control (e.g. geofencing, beacons, cell-tower triangulation).
- Rapid re-issuance of cards following a breach, minimizing user inconvenience.

> See Appendix D on the security of mobile payments for more detail.

Adoption

Charity donations and service charges can be made via carrier networks, and we can NFC (near-field communication) our way across major cities without touching a payment card. In emerging markets, mobile is offering banking opportunities to communities that previously had no access to bank facilities. M-PESA – a banking and payment service based on SMS messaging – is revolutionizing life in India and Africa, and BBM Money is offering a similar service across Indonesia.

Mobile ecommerce (mcommerce) has been a huge growth area, with around 30% of all ecommerce transactions across the US performed using a smartphone or tablet[8]. During the 2015 Christmas shopping period, over 50% of all online transactions in the UK were made on a mobile device[9]. Mobile is penetrating face-to-face transactions too. With mPOS shipments forecast to hit 22 million in 2021, mobile point of sale (mPOS) devices are set to make up an anticipated 45% of all POS terminals in circulation[10].

mPOS has been a boon for small merchants and emerging markets, where it has lowered the barriers to entry for small merchants who want to accept payment cards.

Mobile devices have become an increasing target for malware attacks – mobile applications are notoriously vulnerable to common coding weaknesses – and it is estimated that some nine million devices are lost or stolen globally every year[11]. Poor consumer security awareness only compounds the problem; many mobile device users will connect to public Wi-Fi networks on a routine basis, and most only use simple PIN protection to lock their phones – if anything at all.

Multi-factor authentication is perhaps one of the best personal security measures we can adopt as individuals for our own security, just as much as the payments industry would benefit from the potential it offers in identification and authorization for transactions. Sadly, many users find these cumbersome and inconvenient to use. As long as users do not have to accept responsibility for any fraud conducted against their bank accounts, this situation is unlikely to change.

Convenience is the single most significant benefit our beloved mobile devices give us. Mobile has become such an embedded part of our lives that many public facilities – from shopping malls to theme parks – offer free wireless access. Public Wi-Fi – for all its lovely slick internet-ness – can be a poisoned chalice. A huge proportion of public Wi-Fi networks are insecure, allowing anyone with even the smallest bit of know-how to intercept our transmissions.

It's only a matter of time

While the general consensus is that mobile presents an attractive target to attackers, so far there's little evidence of significant mobile-based attacks. Over the last three years the Verizon DBIR team has analyzed thousands of data breaches and mobile was not identified as a root cause in a single one[2]. Mobile devices are affected by malware, but the vast majority of that is adware and relatively innocuous. Of the tens of millions of devices on the Verizon network, the 2014 DBIR reported that only 0.03% of these were infected with truly malicious exploits. But there is no room for complacency. In ISACA's Mobile Payments Security Survey, 87% of security professionals said they anticipate an increase in mobile payment data breaches over the coming year[12].

Mobile devices as payment terminals

Within the US retail space, Verizon's QSAs have found more merchants are looking to their existing mobile devices to provide additional payment services using "sleds" from payment device manufacturers that slide over the mobile device[11]. Ideally, those sleds offer point-to-point encryption and their own Wi-Fi connections, EMV (made up of the name of its founders: Europay, MasterCard and Visa) and NFC options, and keypads (for connections to acquirers and for manual card entry that is distinct from the mobile platform). When the payment sleds are not P2PE-validated, do not offer Wi-Fi, EMV, NFC or keypad capabilities, and the mobile device platform and its utilities are used to receive and transmit payments, the scope of a PCI DSS assessment increases significantly.

Perhaps one of the biggest challenges presented by mobile is that despite all the concerns from within the security industry, these qualms are not shared by the general public[13], who are only too willing to place their lives under the control of their electronic companion.

Even if patches exist, many devices are never updated by the operators, or are too old to be updated but are used nonetheless. Stagefright, a remote code execution vulnerability in Android that exploited the multimedia playback engine, didn't need any user interaction with the device to be exploited; all an attacker needed was a phone number[14]. Man-in-the-middle attacks are still possible, despite multi-factor authentication (e.g. if an attacker impersonates a website and forwards user-submitted credentials (user ID, password and multi-factor token) to the user's intended website).

> Undoubtedly, the best way to protect payment card data on mobile devices is by first encrypting it with a P2PE solution.

Improving security and compliance

For merchants seeking to deploy mobile payment solutions, Verizon encourages:

- Use of multi-factor authentication and strong passphrases, to prevent unauthorized access to mobile devices. (This element becomes more important when NFC payment credentials are registered on the device.)
- Authenticating, authorizing and logging activity for each entity involved in the transaction pathway.
- Maintaining the Confidentiality-Integrity-Availability triad for payment messages (payloads) and transmission pathways.
- Verifying the encryption status – including algorithm, key strength and rotation – of transmissions.
- Using chain of custody and geofencing to prevent or resolve physical theft of devices.
- From a merchant application perspective, combining multi-factor authentication with geo-location and transactional velocity to detect fraudulent transactions before they are accepted.

Undoubtedly, the best way to protect payment card data on mobile devices is by first encrypting it with a P2PE solution (wherein the decryption keys are not accessible by the mobile device), and a number of solutions cater to this security measure. Not all of them are validated as P2PE devices by the PCI SSC (and are therefore not permitted for scope reduction), but many of them have wide adoption, nonetheless.

In a scenario in which a PCI-validated P2PE solution is not used, and scope reduction is not granted by the acquirer, all PCI DSS requirements will apply. Of the 12 controls in the DSS, the following requirements tend to be the most difficult for mobile, non-Windows platforms to meet (thus resulting in rather creative compensating controls):

- Requirement 5 – Anti-virus (due to the difficulty in administering signature updates and regular device scans).
- Requirement 10 – Logging and time synchronization.
- Requirement 11 – Internal vulnerability scanning, penetration testing and file integrity (or change-detection) monitoring.

OWASP top 10 mobile risks

Recent surveys of popular mobile applications show that a high proportion of them are insecure. The 2016 State of App Security report from Arxan found that 90% of the mobile health and finance apps tested had at least two of the OWASP Mobile Top 10 Risks[15].

M1: Weak server side controls
M2: Insecure data storage
M3: Insufficient transport layer protection
M4: Unintended data leakage
M5: Poor authorization and authentication
M6: Broken cryptography
M7: Client side injection
M8: Security decisions via untrusted inputs
M9: Improper session handling
M10: Lack of binary protections[16]

EMV

Counterfeit cards make up the largest share of card fraud, but the introduction of EMV has significantly reduced the success rate of counterfeit fraud.

The EMV protocol is a deterrent control, making it best suited to maintain the integrity of cardholder data outside of, and before it enters, a merchant's environment. Alone, it cannot secure or prevent the theft of cardholder data within an organization. Because it has no impact on the security of cardholder data within an organization, EMV cannot, for instance, offer any level of scope reduction to merchants that have enabled it. For this level of preventative control, technologies such as P2PE and tokenization are better suited.

Adoption

Most major European nations moved to EMV during the early 2000s. They actually went a step further in their implementation and replaced signatures with PINs, whereas the US went with chip and signature as a more familiar approach to minimize consumer disruption. However, the use of PINs is arguably more secure, as signatures can be easily copied.

Many large retailers – including Walmart, Target and Costco – have upgraded their terminals and are activating them for chip payments, but many smaller retailers have not migrated and many have no plans to do so. Even in locations where chip payments are accepted, only 40% of consumers use this method, with 60% unsure about the new technology[17].

> By 2017, it's expected that more than 97% of cards in the US will be chip-enabled, with significant growth in the number of merchants accepting EMV as well[18].

Why the US is finally moving to EMV

Sharply rising counterfeit card fraud was a key reason why the business case finally began to work for US issuers. Following early EMV adoption, fraud began to fall. According to MasterCard, there was a 54% decrease in counterfeit fraud costs at US retailers that have either completed or are close to completing EMV transitions, as measured between April 2015 and April 2016[19].

Other contributing factors include the increasing difficulty of using magnetic stripe cards overseas, the desire to accelerate the upgrading of the US terminal infrastructure to NFC-based mobile payments technology, and the decreasing cost of chips and terminals.

> EMV is not a panacea that will eliminate all payment card fraud.

Effectiveness

EMV is not a panacea for all card fraud. In the countries where it's been introduced, it has shifted fraud onto card-not-present (CNP) transactions – such as telephone, mail order and online.

To combat ecommerce fraud, 3D Secure has been created as an additional layer of authentication for CNP transactions. There are varying iterations of 3D Secure, from basic to more enhanced versions. The enhanced 3D Secure offerings provide multilayered protection. Cardholders are enrolled in the service automatically, making it an invisible and seamless experience. Looking at Europe's experience, the UK Cards Association reported a one-third drop in CNP fraud since 2007 due to increasing use of fraud screening tools and 3D Secure[20].

The costs associated with implementing EMV in a modern, technology-driven environment eventually have to result in benefits sufficient to cover the fraud costs that migrate to CNP channels, as well as the costs of migration. If this equation doesn't net positive results, little incentive exists for the adoption of EMV.

A 2014 estimate put the average cost of issuing a new EMV card at $3.50. By comparison a magnetic stripe-only card cost around $1 – up to 60% of which was postage. The average cost of a new EMV-compliant point-of-sale terminal was $500 – $1,000[21]. Since then, the cost of EMV terminals has decreased significantly as manufacturers have ramped up production volumes and compete for market share.

The future

Technology has moved on. As a Visa representative commented in CNN money, "[Chip and PIN] will have a shorter shelf life. We're moving to new technologies and innovation."[22]

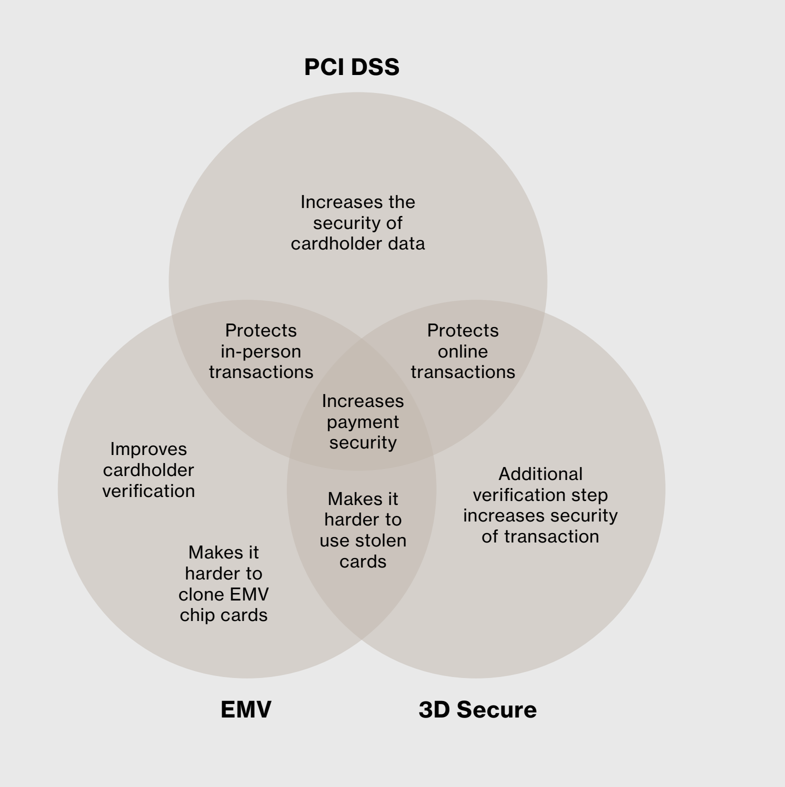

PCI DSS
Increases the security of cardholder data
Protects in-person transactions
Protects online transactions
Increases payment security
Improves cardholder verification
Makes it harder to use stolen cards
Additional verification step increases security of transaction
Makes it harder to clone EMV chip cards
EMV
3D Secure

FIG 5 – How PCI DSS, EMV and 3D Secure combine to improve payment security

P2PE and tokenization

Point-to-point encryption (P2PE) involves the encryption of card data at the point of capture, within the payment terminal. The data remains encrypted until it reaches the payment processor, or other designated end-point. This means that any data intercepted within the merchant's operating environment is useless. Decryption only happens within a separate, properly controlled environment.

Implemented correctly, P2PE can enable merchants to remove some payment card data from the scope of their own PCI DSS compliance. The key determinants are:

- Encryption keys must be protected in hardened payment terminals.
- Decryption keys must be protected in systems not accessible by the environment that performs the encryption: third-party payment processors, third-party P2PE providers, or even managed by the merchant itself.

Tokenization is another approach that can remove card data from a payment transaction. Payment tokens are presented and used instead of the true card data to complete a transaction.

Encryption versus tokenization

Both encryption and tokenization transform cardholder data. Encryption does it with an algorithm, and it's the encryption and decryption keys that must be protected. In tokenization, the transformation is carried out using a database table and randomization, and it's the database table that must be protected.

> “ EMV does not remove the need for P2PE or tokenization.

These solutions take over where EMV leaves off. EMV protects the card data while it's in possession of the cardholder; PCI DSS, PCI PA-DSS, PCI P2PE and tokenization protect it throughout the payment lifecycle.

Who benefits?

P2PE and tokenization benefit merchants first, issuing banks and card brands second, and, finally, acquirers. Merchants profit from a reduction in PCI compliance costs (in most implementations) and the reduced likelihood of reputation- and revenue-damaging data breaches. Issuing banks and card brands benefit from reduced cardholder data fraud. Acquirers benefit from new P2PE and tokenization service revenue streams, as well as reduced risk portfolios, in their mandated reporting to the card brands.

More merchants are turning to P2PE vendors and either acquirer-issued tokens or third-party tokenization vendors. Yet, the number of PCI-validated P2PE vendors has not kept pace. At the time of writing, only 24 such solutions are listed on the PCI SSC website; notably absent from them are some of the most popular – and often bank-endorsed – offerings.

Biometrics present a big opportunity to update existing card formats for both convenience and security.

The reason for the discrepancy is the purported difficulty in meeting the P2PE standard issued by the PCI SSC. The fact that the retail industry needed a solution like P2PE before the PCI SSC caught up with how to make the market offerings adhere to a sanctioned level of compliance is an interesting case of security leading compliance. Among the players wrestling with some of the resultant tension are: acquirers that often sold the non-PCI-validated P2PE/tokenization solution; merchants that bought the solution, thinking it guaranteed a reduction in PCI compliance scope; the PCI SSC, which officially only permits scope reduction using solutions validated against its standards; and the QSAs, who are trying to verify the scope and compliance of merchant environments.

> It remains to be seen whether the major players in the P2PE market yield to the rigors of P2PE validation assessments, or the P2PE standard is revised to make attaining compliance more achievable.

PCI SSC has clarified that PCI qualified assessors may work with acquirers to recommend the extent to which a particular non-PCI validated P2PE implementation may or may not offer sufficient security to qualify for a reduction in PCI DSS scope. The acquirer can then decide to accept, ask questions, or determine the approach is not acceptable[23].

What’s next?

Looking at the mainstream press you’d think that it was all about blockchain and bitcoin. But according to figures from Capgemini, virtual (or crypto) currencies only make up a tiny fraction of the hidden payments market – which itself is only a small fraction of non-cash transactions[24].

Category	Transaction volumes (billion)	
	Lower range	Higher range
Closed loop cards/mobile apps	15.1	22.6
Digital wallets	8.2	16.5
Mobile money	1.1	1.8
Virtual currencies	0.03	0.04
Total	24.5	40.9
Hidden market as percentage of estimated non-cash transaction volumes in 2014	6.3%	10.5%

FIG 6 – Hidden payments market estimation, Capgemini[25]

Closed loop systems and mobile apps have made much greater inroads into replacing payment card transactions.

Biometrics present a big opportunity to update existing card formats for both convenience and security. MasterCard is already trialing cards with a built-in fingerprint scanner. Zwipe promises the convenience of contactless payments, but without the transaction limit – typically $25 – 50. And the good news for merchants is that this wouldn’t require yet another refresh of POS terminals.

Fintech and new entrants are disrupting the payments industry, but the market is highly fragmented and cards are likely to dominate for a while to come – remember, checks are still around.

Section 4:
Data breach comparison

Despite advances in the state of global compliance, many companies are still struggling with achieving and maintaining data protection. Attackers can exploit systems in just minutes, while defenders often take weeks or more to discover breaches. With no slowdown in sight, the effectiveness of the PCI Security standards, and PCI DSS in particular, continues to be a hot topic.

Verizon has been playing a key role in the fight against cybercriminals since the 1990s. Each year, our security reports – including the DBIR, the Data Breach Digest, The Protected Health Information Report and the Payment Security Report – provide valuable information to help protect your organization.

> “ Each year, the Verizon DBIR provides insight into the global threat landscape based on analysis of thousands of confirmed data breaches. This includes who the threat actors are, the motivation behind the attacks and the methods used[2].

Since 2010, we’ve compared the state of PCI DSS compliance in organizations undergoing interim validation versus those being assessed following a confirmed data breach. In the 2015 PCI Report, we emphasized that the effectiveness of payment card data protection is mostly determined by the approach taken in implementing and maintaining the set of PCI DSS controls.

Compliance correlation trends

Forensic investigators accredited by the PCI SSC to conduct the formal data breach investigations are often tasked with helping the victim organization contain the breach, confirm its extent and, if possible, identify the origin of the perpetrator. Sometimes some aspects of a control failure are made known, but the details and exact nature of the failure are seldom, if ever, disclosed externally. While understandable, this unfortunately limits the learning opportunity.

Our analysis compares the state of PCI DSS compliance at the time of a breach (as determined by Verizon’s PCI Forensic Investigators) with that of a control group (as assessed by Verizon QSAs during interim compliance validation). The data provided by Verizon’s Forensic Investigation practice is from cases that involved confirmed compromise of payment account data. None of Verizon’s PCI customers have reported a payment card compromise after being assessed by Verizon and thus are not included in the confirmed compromise data set.

Each year we see very clear indicators and correlations between these two data sets. Our analysis identifies common breach vectors and extrapolates the control(s) that would prevent similar breaches from being successful.

There are significant differences between the scope and intent of a forensic investigation and PCI DSS compliance validation. Whereas a QSA would dive into the specifics of each control and testing procedure, a PCI Forensic Investigator’s (PFI) task is to make a high-level assessment as to whether the organization was compliant with each of the 12 PCI DSS Key Requirements at the time of the breach. The PFI doesn’t attempt to validate compliance (a positive), but rather looks for non-compliance (a negative). Given this, it’s likely that the PFI data will show a more optimistic picture of compliance.

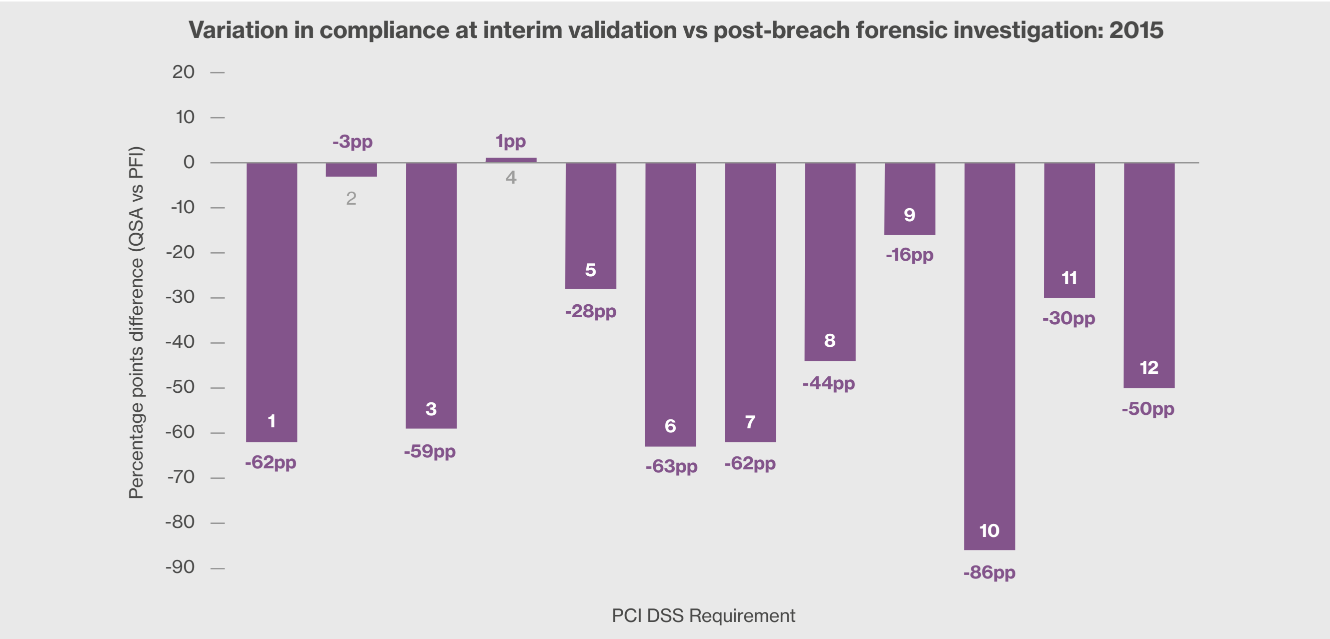


FIG 7 – QSA versus PFI. PFI data does not indicate the data breach cause. It includes "partial yes" responses (not indicative of full compliance).

Comparison between QSA and PFI

The figure above shows that compliance with most PCI DSS Key Requirements is significantly lower in post-breach assessments by PFIs than in interim validation assessments by QSAs – this despite the fact that PFI investigations are less critical than a formal QSA validation.

The difference is expressed as a negative percentage point. It indicates the average PCI DSS compliance difference between the two data sets, i.e. between breached organizations (mostly non-PCI DSS attested) and the "control group" from our set of interim PCI DSS attested organizations.

Note that the 2015 PFI data set covers a different caseload of data breaches to those that were investigated in 2014. That makes the ongoing similarities in compliance trends, with year-over-year comparison of this data correlation, even more striking. It strengthens our finding that breached organizations clearly demonstrate a predictable pattern of behavior.

Overall, breached organizations have significantly lower compliance – there's a 42 percentage point difference in total average PCI DSS compliance. Between 2014 and 2015, this gap in compliance increased for two Key Requirements: Requirement 1 by 20 percentage points; Requirement 3 by 33 percentage points.

The only requirement where breached organizations actually scored slightly better (by 1 percentage point) was Requirement 4.

The 2014 report revealed that not a single breached organization had Requirement 6 or Requirement 10 in place at the time of being breached. In 2015, at least some of the breached organizations were found to have these requirements in place.

However, with 86 percentage points difference, Requirement 10 still has the largest difference between our two groups. Where organizations continue to exhibit poor logging and monitoring, breaches often go undetected for months or years.

Comparison with previous years

In our 2015 report we found that organizations experiencing data breaches in the previous year fell down in PCI DSS compliance in five main areas:

- Develop and maintain secure systems (Requirement 6)
- Restrict access (Requirement 7)
- Track and monitor access to networks and cardholder data (Requirement 10)
- Test security systems and processes (Requirement 11)
- Maintain an information security policy (Requirement 12)

Overall, organizations experiencing a data breach were less likely to be compliant with 10 out of the 12 PCI DSS Key Requirements.

> Organizations that do not maintain an industry-accepted baseline set of security controls have significant increased exposure to data breaches.

Being fully compliant with PCI DSS does not guarantee security – although it certainly helps. Compliance enables security. To date, no breached organizations that requested support from the Verizon RISK Team were found to be fully compliant at the time of breach. Were a breach on a compliant entity to occur, it likely would indicate circumvention of multiple control layers by the attackers and/or exploitations of ineffectively implemented controls – and it would make a fascinating case study.

> Of all the payment card data breaches that the Verizon RISK Team investigated over the past 11 years, not a single organization was fully PCI DSS compliant at the time of the breach.

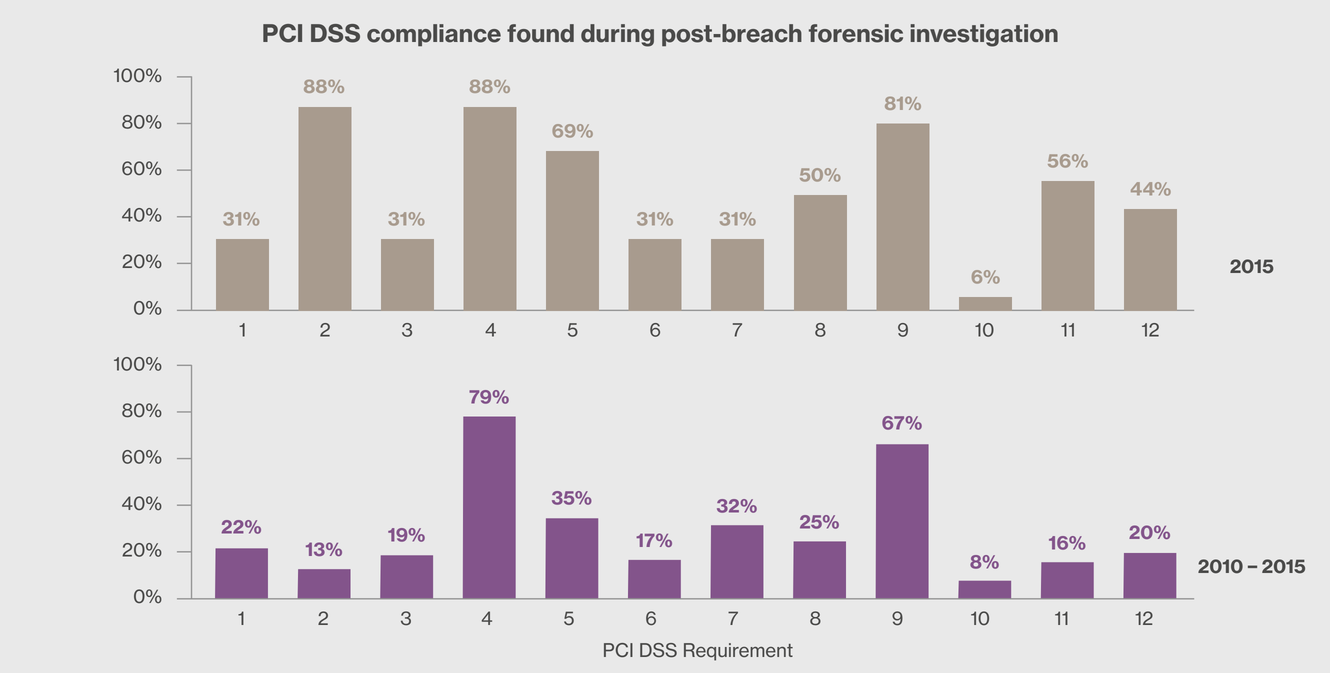


FIG 8 – PFI compliance, 2010 – 2015. Data includes "partial yes" responses (not indicative of full compliance with PCI DSS).

> If your organization doesn't do a good job patching, maintaining and monitoring key systems, you just might find yourselves on the wrong side of next year's analysis.

Section 5: Recommendations

Most companies initiated their PCI Security compliance programs many years ago. By now, they certainly should have processes in place to support their program; making daily management and ongoing control maintenance relatively effortless. Sadly, that's not always the case.

The PCI DSS is not a risk management standard. It does not provide prescriptive recommendations that specify how to identify, treat or manage risk – which is fine. Its goal is to provide a minimum set of general controls that, when implemented correctly and consistently maintained, provide reasonable assurance that payment card data is secure.

> “ Protecting information, no matter where it is located, requires a fundamental shift in focus. Information security professionals who are accustomed to concentrating on technology need to switch gears and focus on business processes and data[26].

Monitoring control effectiveness against exposure to risk is key to achieving security through compliance. Yet the requirement for this kind of control monitoring is starkly missing from the PCI DSS. The PCI DSS does not assess methods used by organizations to evaluate the effectiveness of controls in operation. The lack of ongoing control evaluation contributes to the ‘check-box’ mentality that some organizations have toward PCI DSS compliance.

Controls can satisfy compliance validation criteria without explicit evidence that control effectiveness was also evaluated. The assumption is that controls will be effective by presence alone. This is why it has become so essential that control effectiveness guidelines be included in the PCI DSS.

You cannot evaluate overall control effectiveness without also measuring its contribution toward risk mitigation. Controls should only be considered effective when their contribution to the control system and control environment mitigates risk to an acceptable level.

The PCI DSS continues to evolve, making it easier for organizations to understand what “doing the right things” means, how to go about doing it and when to do it. But in its current form, it may benefit from including guidance on aspects such as:

- How organizational involvement in control design impacts control effectiveness, resilience and sustainability.
- How a control operates within a control system where controls have interrelated dependencies.
- How control performance is directly influenced by the environment in which it operates.

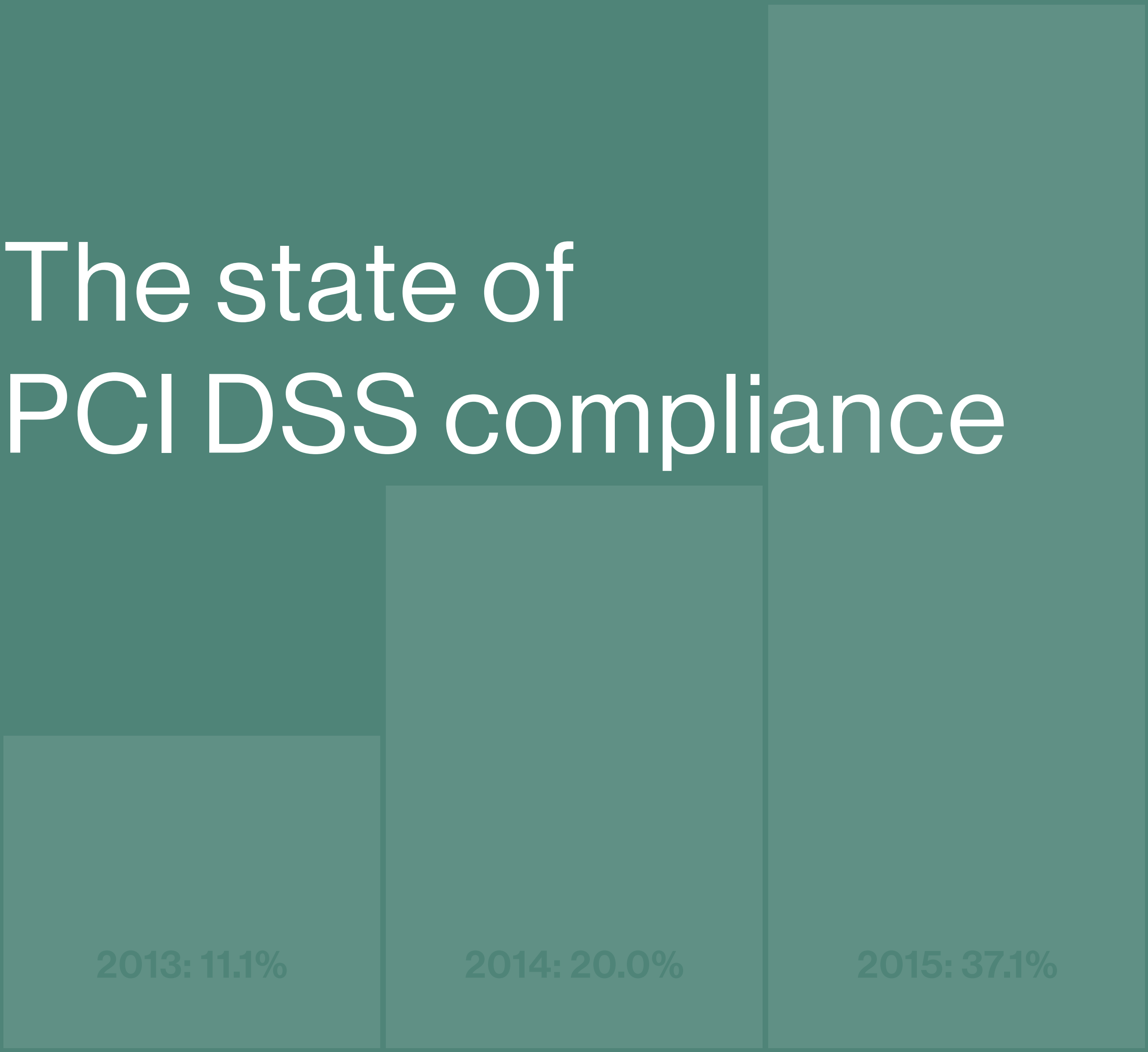
Without conscious consideration of these aspects during their implementation, the ability of a control to successfully mitigate risk on a continuous basis will be compromised; it will be sustainable merely by luck – certainly not by design.

The answer is to go back to basics and:

- Refocus the discussion around control effectiveness and risk mitigation.
- Acknowledge the necessity of an industry-defined/guided risk-based approach to understand effective control management.
- Broaden guidance on control design and implementation, and encourage development of intelligent control systems.

This is no easy task, but it is critical to developing a robust, sustainable and secure payment industry.

The state of PCI DSS compliance



1 Install and maintain a firewall configuration

2 Do not use vendor-supplied defaults

3 Protect stored cardholder data

4 Protect data in transit

5 Protect against malicious software

6 Develop and maintain secure systems

7 Restrict access

8 Authenticate access

9 Control physical access

10 Track and monitor access to networks and cardholder data

11 Test security systems and processes

12 Maintain an information security policy

The state of PCI DSS compliance

Full compliance

Organizations are required to achieve and maintain a 100% state of compliance, where all applicable security controls continuously remain in place. We measured organizations across our global PCI DSS assessment data set, to determine for each Key Requirement the percentage of organizations that scored 100% during iRoC assessment.

Conducting an independent interim compliance validation assessment several months before the scheduled annual final assessment provides the best opportunity to identify organizations that keep all their security controls in place throughout the year (actual full compliance). It also highlights organizations that allow controls to fall out of place, by giving them attention only at the end of the compliance validation cycle in order to achieve a clean annual assessment.

The control gap

As well as compliance by organization, we also looked at average compliance. We worked this out by looking at all controls, and testing procedures under a particular requirement, and dividing the number that passed by the total. Comparing this data with the compliance by organization (full compliance) provides some interesting insights. It allows us to identify the proportion of PCI DSS controls that organizations are struggling to comply with.

We have been tracking the control gap since PCI DSS 1.1. In our previous reports (the Verizon 2014 and 2015 PCI Reports), we explained how each update to the PCI DSS impacted organizations' ability to meet the requirements. The control gap data for 2015 is based on PCI DSS 3.0 and 3.1 assessments conducted worldwide in 2015.

Full compliance continues upward progression

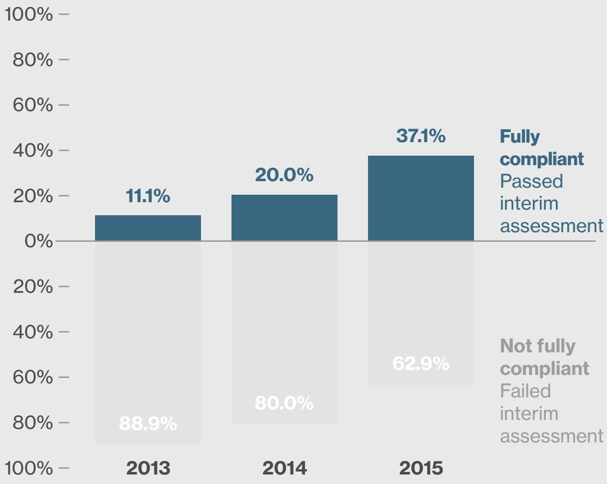


FIG 9 – Overview of full compliance at iRoC 2013 – 2015

But the control gap has widened

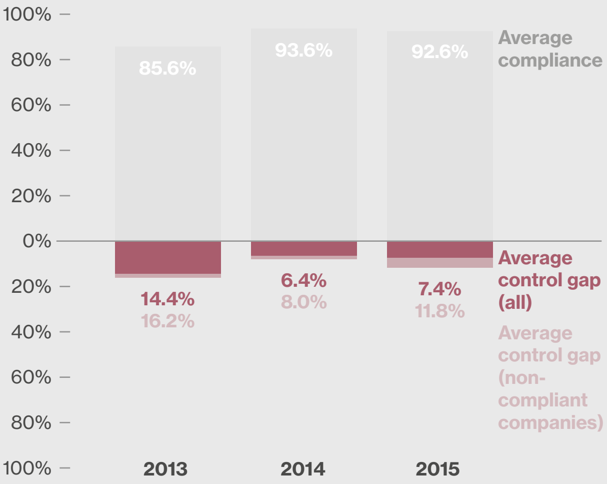


FIG 10 – Overview of average control gap 2013 – 2015

Summary of PCI DSS compliance by Key Requirement

Full compliance

The most compliant 100% requirement was “Protect against malicious software” (Requirement 5), which 90% of all organizations managed to keep in place. Requirements 1, 6, 11 and 12 were the least sustained, with only 70% of organizations achieving 100% on those requirements.

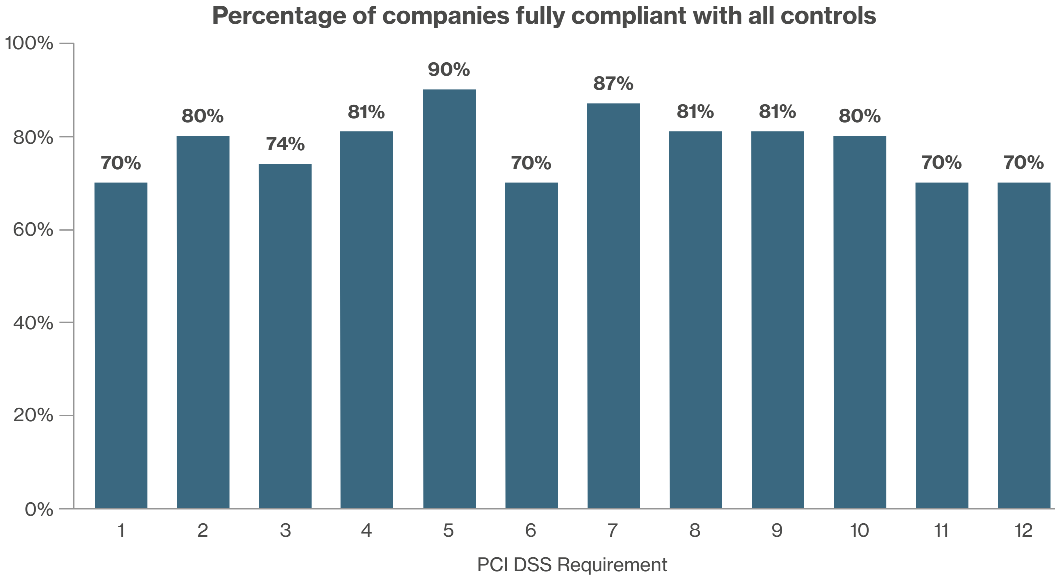


FIG 11 – Full compliance by Key Requirement at iRoC 2015

Control gap

While five Key Requirements (5, 8, 9, 11 and 12) improved between 2014 and 2015, 58.4% of controls declined in compliance. Requirements 4 and 11 have the largest control gap.

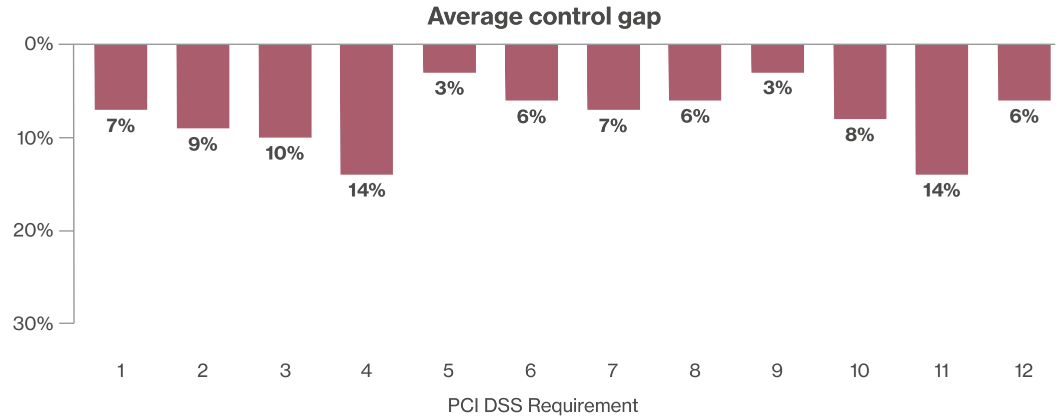


FIG 12 – Average control gap by Key Requirement at iRoC 2015

Compensating controls

Requirements 8, 2, 3 and 1 are compensated the most – unchanged from 2014. No organizations applied a compensating control under Key Requirements 4 or 7.

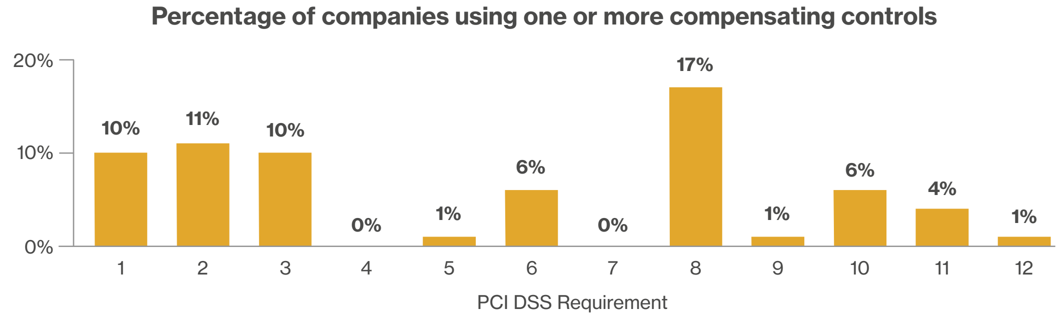


FIG 13 – Use of compensating controls by Key Requirement at iRoC 2015

Key Requirement 1:
Install and maintain a firewall configuration

Requirement 1 covers the use of a firewall to filter traffic between defined perimeters – internal to external networks, cardholder data environment to corporate LAN etc. As well as maintaining filters that specify the types of network traffic permitted across boundaries, organizations must have a mature process for documenting, testing and approving new connections and changes to existing ones.

The Verizon DBIR shows that sensitive assets (e.g. POS terminals) are often compromised following an initial intrusion into less sensitive network areas. The ability of an organization to segment its network and apply granular traffic filters is vital for breach prevention and containment.

Key findings

- Over two-thirds of organizations fully met Requirement 1 at interim assessment. This ranks it among the lowest for compliance sustainability – after 6, 11 and 12.
- Compliance against every control declined.
- Organizations struggled most with control 1.4 (Install personal firewall) – where the average control gap was 11.8%.
- 1.4 also saw the greatest use of compensating controls within Requirement 1 – 3.5% of organizations used one or more compensating controls to meet it.
- Organizations in North America applied compensating controls for Requirement 1 twice as often as those in Europe and Asia-Pacific regions.
- Service providers (93.4%) slightly outperformed merchants (92.2%) for full compliance.

Proportion of companies fully compliant

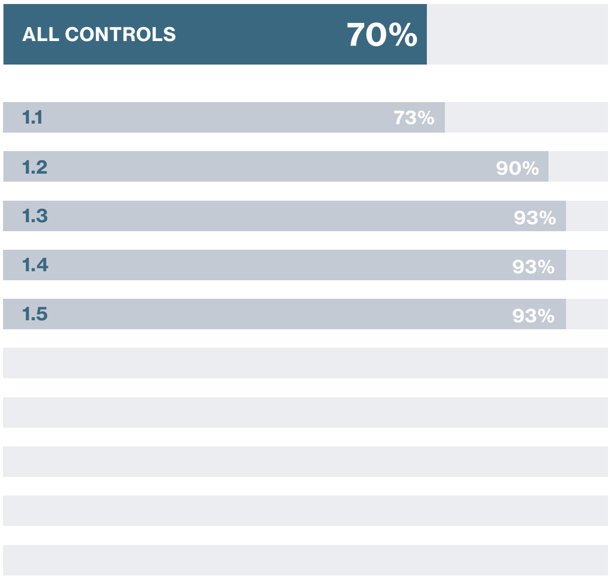


FIG 14 – Requirement 1: % organizations fully compliant

Average control gap

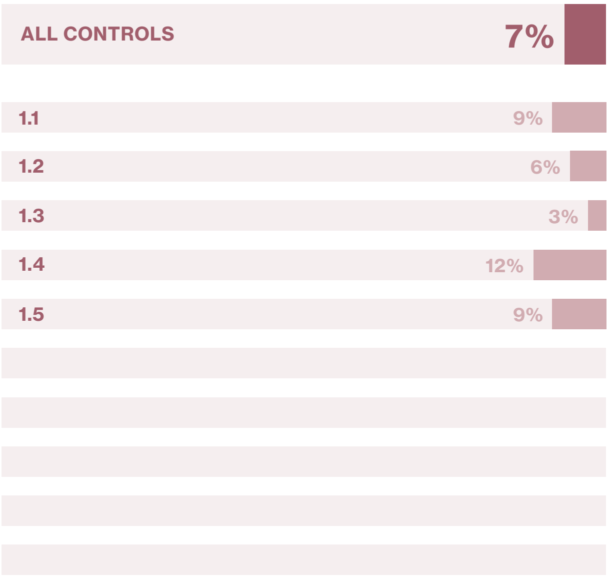


FIG 15 – Requirement 1: average % of controls not in place

All industries 70%

Retail and hospitality 67%

The average control gap in the retail and hospitality industries was 7.6%. The poorest performance was for control 1.4, where the average control gap was 11.8%. Retail and hospitality companies have some of the largest workforces in the economic machine, making the management of personal devices – often on a national network of locations (be it hospitals or outlet malls) – challenging without the use of enterprise device management tools.

Financial services 67%

The financial services industry was outperformed by the other sectors for Requirement 1, with an average control gap of 10.9%. Financial services organizations struggled most with control 1.5 (Documented policies and procedures for managing firewalls), with a control gap of 26.7%. Their focus is on their financial solutions, products and consultancy services. And they can find it hard to lock down the time or resources to adequately document their network and the tech that runs it.

IT services 83%

IT services was the best-performing industry in Requirement 1, with full compliance of 83% and a control gap of 3.5%. It achieved 100% compliance with control 1.5. It struggled most with control 1.4, where the control gap was 13.3%.

> Protect the rest of your network from compromised desktops and laptops by segmenting the network and implementing strong authentication[2].

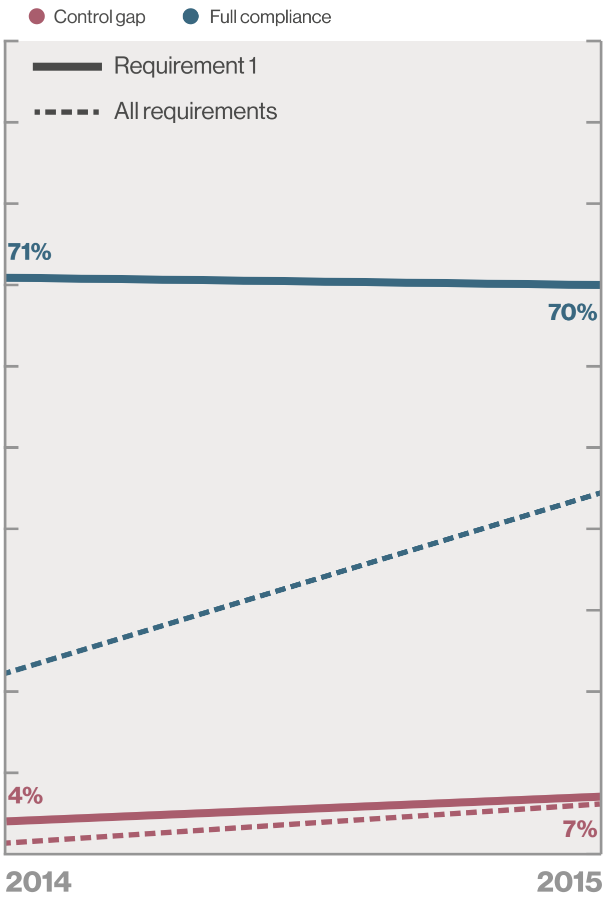
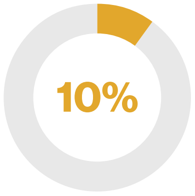


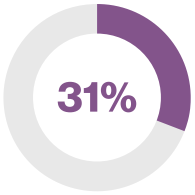
FIG 16 – Requirement 1: 2014 – 2015 comparison

Year-over-year comparison

Full compliance with Requirement 1 remained relatively unchanged in 2014. The control gap increased from 4% in 2014 to 7% in 2015, as some companies found it more difficult to maintain compliance. But the proportion of the organizations using compensating controls declined significantly. One in 10 organizations used them in 2015, compared to a third in 2014.



10% of organizations used one or more compensating controls for Requirement 1 in 2015, down from 33% in 2014.



31% had Requirement 1 in place at the time of a breach—up from 27% in 2014.

Key Requirement 2:
Do not use vendor-supplied defaults

The aim of Requirement 2 is to prevent malicious individuals exploiting default configurations and passwords. Organizations are required to create standards that are consistent with industry-accepted system-hardening standards, deploy those standards to wired and wireless devices, and protect remote non-console administrative access to systems and applications.

These requirements feature prominently in the milestones of the PCI Prioritized Approach. Those companies still using SSL and early TLS versions, all of which are now considered insecure, and in the process of implementing secure TLS versions, will find additional testing requirements for control 2.3.

Key findings

- 80% of companies assessed in 2015 were fully compliant at interim assessment. The control gap was 9.1%.
- The weakest performance was in control 2.2 (Develop configuration standards for all system components). This was one of the worst-maintained controls, ranking 19th from the bottom of all controls.
- Companies that elected to use DSS 3.x in 2014 were ready for the new control 2.4 (Maintaining an inventory of in-scope systems) – average compliance with this control was 100%. But in 2015, there was a control gap of 4.8%. This could indicate that companies that had their first DSS 3.x assessment in 2015 could have made better preparations.
- Control 2.1.1 (Changing wireless vendor defaults) was among the least compliant controls in the Europe and Asia-Pacific regions.
- Around one in 10 organizations used compensating controls for Requirement 2. Control 2.3 (Implement only one primary function per server) required the most compensating controls in North America.

Proportion of companies fully compliant

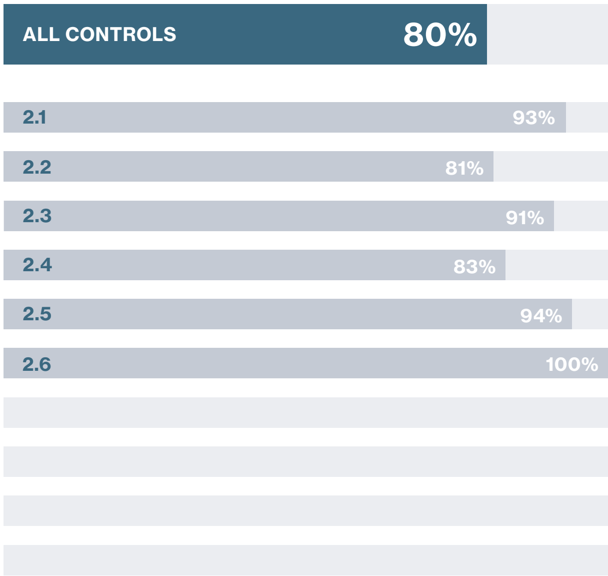


FIG 17 – Requirement 2: % organizations fully compliant

Average control gap

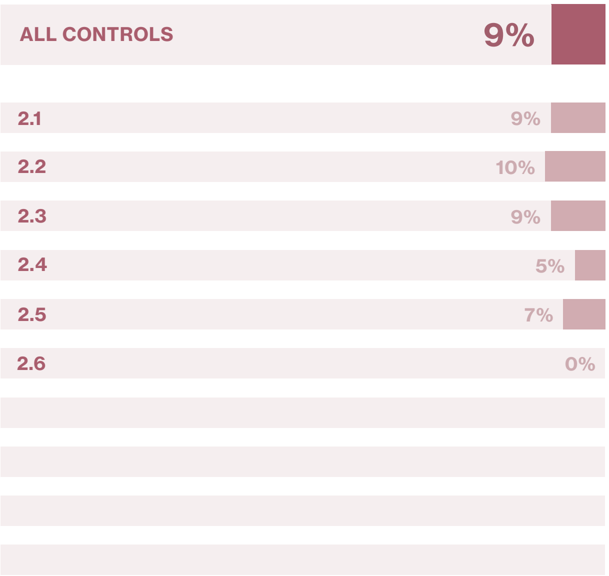


FIG 18 – Requirement 2: average % of controls not in place

All industries 80%

Retail and hospitality 76%

The retail and hospitality industries had a control gap of 7.6% for Requirement 2. Three of the controls (2.4, 2.5 and 2.6) were fully met. The most challenging control was 2.2 (Develop configuration standards for all system components). Retail and hospitality organizations operate at margin (more so than most others), and having a store or property up and generating revenue often takes priority over documenting system security.

Financial services 75%

The financial services industry had the poorest performance of all the industries on Requirement 2, with a 17.2% control gap. This is the requirement with which this industry is struggling the most, mainly due to issues around control 2.3 (Encrypt non-console administrative access).

IT services 100%

IT services outperformed all other industries and achieved 100% compliance. After all, their livelihood depends upon it, as breaches to their systems are breaches to customer services and information that extends beyond cardholder data. We are curious to see if this industry can maintain this perfect score in years to come.

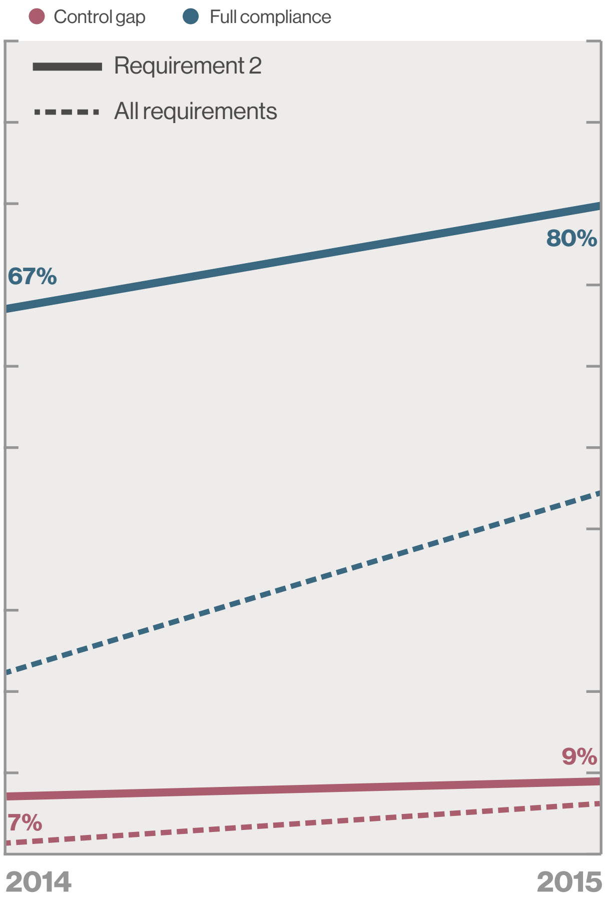
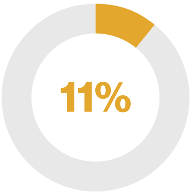


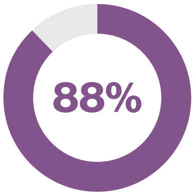
FIG 19 – Requirement 2: 2014 – 2015 comparison

Year-over-year comparison

The proportion of organizations achieving full compliance with Requirement 2 in 2015 increased by 13 percentage points on 2014. But the control gap also grew. The proportion of organizations using compensating controls fell significantly.



11% of organizations used one or more compensating controls for Requirement 2 in 2015, down from 41% in 2014.



88% had Requirement 2 in place at the time of a breach—up from 64% in 2014.

Key Requirement 3: Protect stored cardholder data

Requirement 3 aims to protect cardholder data “at rest” within electronic systems (e.g. database table, application log, or system file), including Sensitive Authentication Data (SAD). There are four main control areas:

- Do not retain cardholder data longer than needed and securely delete cardholder data exceeding defined retention periods.
- Do not store SAD (except for issuers and companies that support issuing services), even if SAD data is encrypted.
- Render data “at rest” unreadable.
- Make sure proper key management procedures are in place to protect both data-encrypting keys (DEKs) and key-encrypting keys (KEKs).

Key findings

- Almost three-quarters of organizations achieved full compliance with Requirement 3 at interim assessment.
- Requirement 3 ranked 8th overall in terms of full compliance, suggesting ongoing challenges to managing, protecting and securely deleting data at rest.
- Requirement 3 ranked second in terms of the proportion of controls that saw the use of compensating controls. 9.9% of controls for 3.4 (Render PAN unreadable anywhere it is stored) needed compensating controls.
- Requirement 3 ranked third-last for both service providers and merchants, in terms of average compliance.

Proportion of companies fully compliant

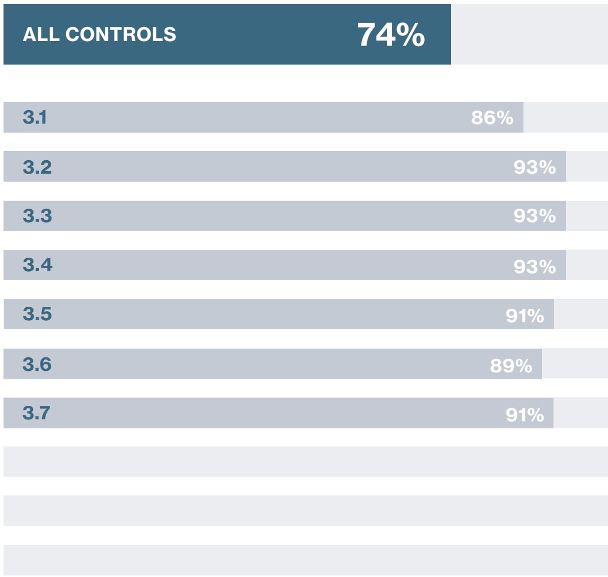


FIG 20 – Requirement 3: % organizations fully compliant

Average control gap

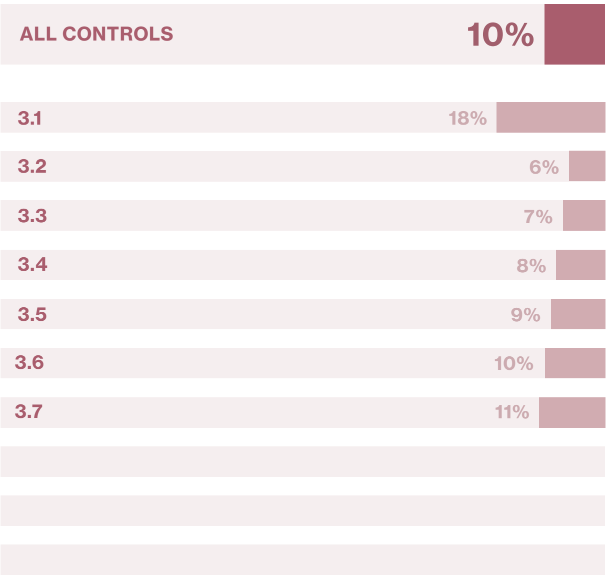


FIG 21 – Requirement 3: average % of controls not in place

*** All industries 74%**

Retail and hospitality 81%

The control gap in retail and hospitality was 4% for Requirement 3. Control 3.1 (Data retention and disposal policies) proved the most challenging – 86% of organizations met this at their interim assessments. Many hospitality organizations were already required to keep certain data for seven or more years, which can sometimes be utilized for PCI DSS – but this may not be documented fully and can require additional scrutiny from the QSA.

Financial services 75%

The financial services industry was outperformed by all other industries for Requirement 3, with a control gap of 14.4%. Financial organizations have more cardholder data, larger PCI scope and far more mainframe systems (like IBM z Systems, HP Integrity NonStop, Stratus VOS and others), which have historically lagged with implementation of encryption and tokenization technologies. They found controls 3.5 (Protect keys used to secure stored CHD against disclosure), 3.6 (Key management procedures) and 3.7 (Policies and operational procedures for protecting stored cardholder data) the most challenging.

It isn't just financial services that struggle with key management. Organizations, in general, find it hard to provide adequate staffing with the right technical know-how. But it shouldn't be taken lightly – it's one of the most important aspects of encrypting cardholder data.

IT services 83%

The IT services industry had a compliance gap of 2.1%. The most challenging controls for IT services companies were 3.6 and 3.7. Sometimes key management processes have been in place so long it can prove hard to lock down the right personnel to document them.

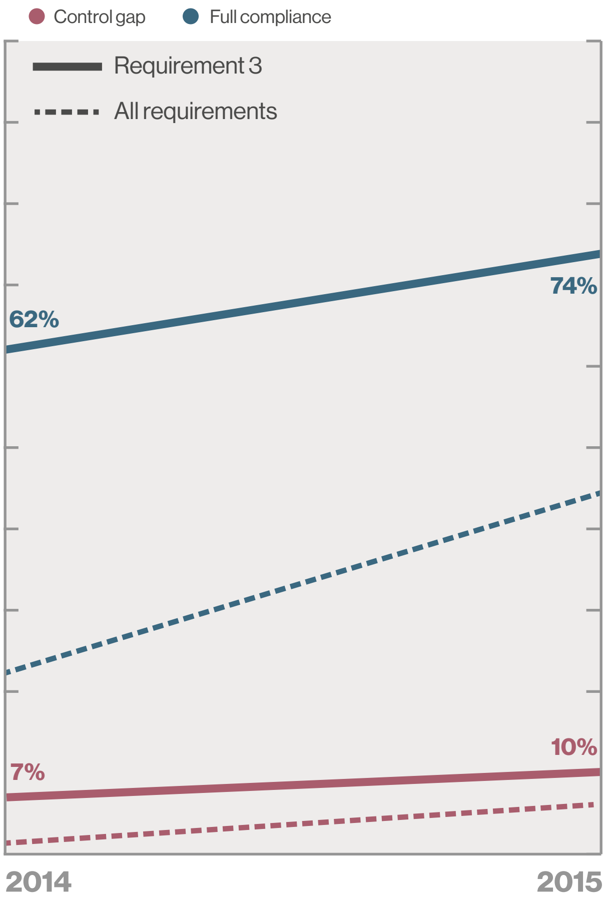
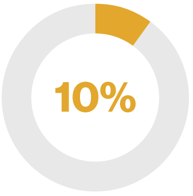


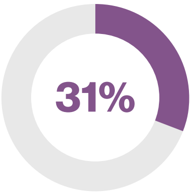
FIG 22 – Requirement 3: 2014 – 2015 comparison

Year-over-year comparison

There was a familiar story for Requirement 3 in terms of year-over-year comparisons. The proportion of organizations achieving full compliance at interim assessments increased, but the control gap widened.



10% of organizations used one or more compensating controls for Requirement 3 in 2015, down from 48% in 2014.



31% had Requirement 3 in place at the time of a breach—down from 36% in 2014.

Key Requirement 4:
Protect data in transit

Requirement 4 is designed to protect cardholder data and sensitive authentication data transmitted over unprotected public networks, such as the internet, where it could be intercepted by attackers.

Key findings

- Four in five organizations maintained year-round compliance with Requirement 4.
- There was a significant year-over-year growth in the control gap of 11.2 percentage points.
- All Asia-Pacific organizations within our data set managed to achieve full compliance – compared with three-quarters of those in North America and Europe. This could be partly explained by Asia-Pacific organizations having introduced payment systems more recently and having fewer issues with legacy systems using weak cryptography.
- Control 4.1 (Use strong cryptography and security protocols) and 4.1.1 (Wireless networks use best practices/do not use weak encryption) were both in the “Bottom 20” of non-compliant controls in North America. 4.1.1 is also in the “Bottom 20” for Europe.
- Control 4.1.1 had the worst record of compliance in North America of all 405 test procedures.
- As in 2014, no compensating controls were used under Requirement 4.
- Across the PCI DSS, Requirement 4 was the most challenging for service providers, with a compliance gap of 16.6%. By contrast, the control gap for merchants was 8.2%. This could reflect the relative complexity and dependency of payment systems within a typical service provider and merchant environment.

Proportion of companies fully compliant

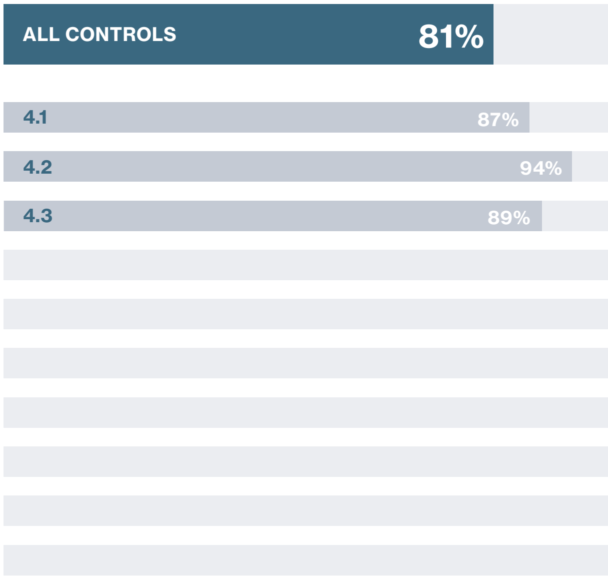


FIG 23 – Requirement 4: % organizations fully compliant

Average control gap

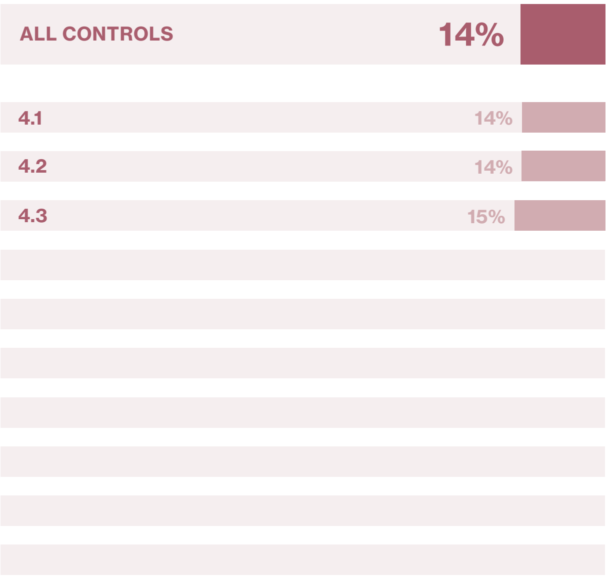


FIG 24 – Requirement 4: average % of controls not in place

All industries 81%

Retail and hospitality 81%

The average control gap in retail and hospitality was 14.2%. Organizations encountered most difficulty with controls 4.1 (Use strong cryptography and protocols) and 4.2 (Never send unprotected PANs by end-user messaging).

Financial services 75%

Three-quarters of financial services organizations were fully compliant with Requirement 4 at their interim assessment. The control gap in 2015 was 15.9%. The worst performance was in control 4.3, where 20.8% of controls were found to not be in place on average. It's important to remember that you are responsible for customer data while it is in your possession, and properly configuring systems that directly handle cardholder data is paramount.

IT services 83%

Surprisingly, the IT services industry was outperformed by all other industries. The industry-wide average control gap (i.e. the average percentage of controls found not in place) on Requirement 4 was 24.1%. While it achieved full compliance with 4.3, it struggled with controls 4.1 and 4.2 – less than three-quarters of these controls were in place on average. Many companies may not go past the initial configuration of servers that are in charge of, or directly interact with, cardholder data. Extra security measures should be in place to verify that any transmissions are sufficiently encrypted.

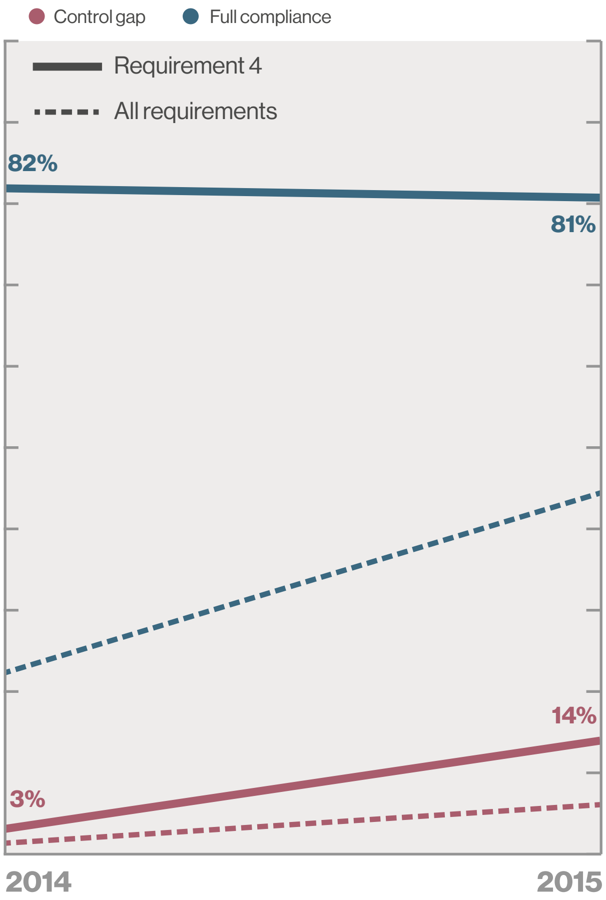
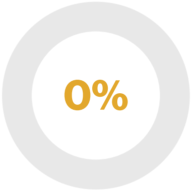


FIG 25 – Requirement 4: 2014 – 2015 comparison

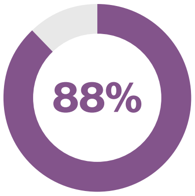
Year-over-year comparison

There was a significant growth in the control gap of 11.2 percentage points between 2014 and 2015. The largest contributor to this was control 4.1, where compliance declined by 12.7 percentage points.

How can we explain this decline in performance? PCI DSS 3.1 introduced a greater focus on the versions of SSL/TLS implemented. To provide this additional level of information to their QSAs, organizations had to look in greater detail at their environments. It's possible that as they carried out more detailed reviews of the transmission of cardholder data (CHD), they uncovered previously unidentified transmissions.



Again in 2015, no companies used a compensating control within Requirement 4.



88% had Requirement 4 in place at the time of a breach—down from 91% in 2014.

Key Requirement 5:
Protect against malicious software

Having malicious software detection in place is key to preventing attackers from using malware to gain a foothold and obtaining unauthorized access to data.

Organizations seldom experience difficulty in meeting the anti-virus controls set out in Requirement 5. In 2015, 90% of organizations demonstrated that they maintain all of these controls throughout the year.

Key findings

- Requirement 5 ranked first out of the 12 Key Requirements for full compliance and is the most sustainable control across the DSS in both North America and Europe.
- Most organizations achieved 100% or near 100% compliance against most Requirement 5 controls. This is possibly due to the ready availability of suitable software and the frequent references to malware in the press and other news sources.
- None of the controls under Requirement 5 appears in our “Bottom 20” list of least compliant controls.
- Compensating controls were only used for control 5.1 (Deploy anti-virus software).
- There was a slight year-over-year decline of 1.8 percentage points in average performance against control 5.3 (Ensuring that anti-virus is actively running and cannot be disabled); all other controls saw improvements in average performance.
- Merchants saw their strongest performance across all 12 Key Requirements in Requirement 5. Just 2% of controls were found not to be in place on average. Requirement 5 ranked second in terms of performance for service providers.

Proportion of companies fully compliant

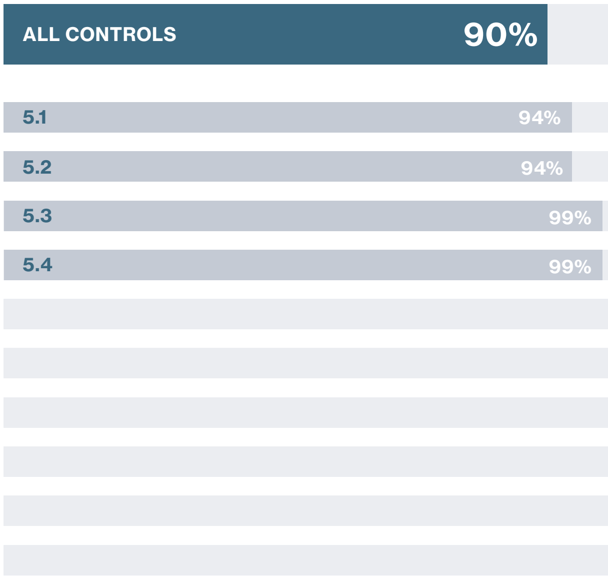


FIG 26 – Requirement 5: % organizations fully compliant

Average control gap

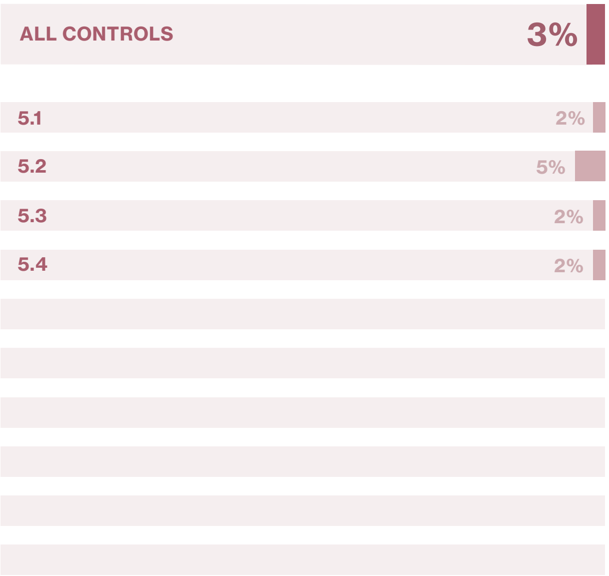


FIG 27 – Requirement 5: average % of controls not in place

All industries 90%

Retail and hospitality 95%

The average control gap in retail and hospitality was very low at 0.5% for Requirement 5. All base controls were fully met, except 5.1 (Deploy anti-virus software), where 1.9% of controls weren't in place on average. Retail and hospitality have hundreds of workstations and servers, which they're constantly adding to, and that can be hard for even the best teams to manage in a compliant fashion. And with so many systems being deployed around the world by various teams, achieving consistency among implementations can be difficult.

Financial services 88%

The financial services industry kept an average of 95.5% of controls in place under Requirement 5, but was still the industry with the lowest performance for this requirement. It performed worst on control 5.2 (Maintain all anti-virus mechanisms). 92% of financial service organizations met this control at interim assessment; across the other industries, all organizations were fully compliant. The issue in financial services may be where companies have deployed more than one anti-virus solution or a mixture of versions. A team is best suited to manage one solution that is centrally managed from a master server. This then updates and enforces policies across all other relevant systems.

IT services 100%

The IT services industry had all Requirement 5 controls in place.

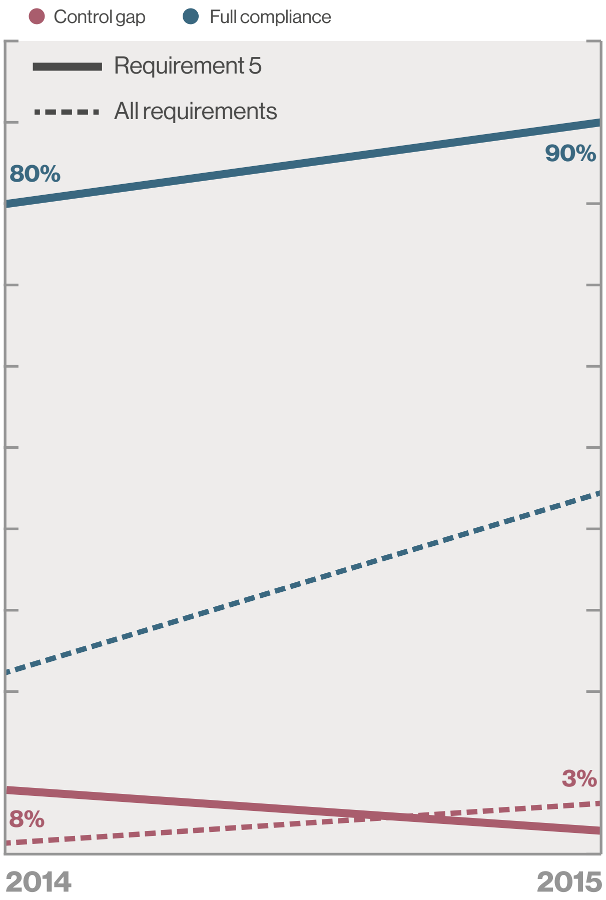
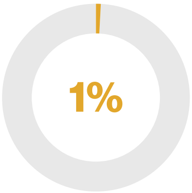


FIG 28 – Requirement 5: 2014 – 2015 comparison

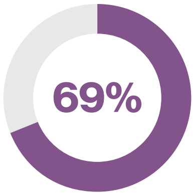
Year-over-year comparison

Average compliance with the anti-virus requirements improved 4.9 percentage points year-over-year. In 2015, it was the control most in place on average; it ranked fourth out of the 12 Key Requirements in 2014.

Performance improved against all controls except 5.3, where the control gap widened year-over-year by 1.8 percentage points.



1% of organizations used one or more compensating controls for Requirement 5 in 2015, down from 15% in 2014.



69% had Requirement 5 in place at the time of a breach—up from 36% in 2014.

Key Requirement 6:
Develop and maintain secure systems

Requirement 6 covers the security of systems and applications, including change management and security patching. It governs how systems and applications are developed and maintained – whether by the organization or third parties. It also recognizes that the threat landscape is always changing and that compliance measures need to be adapted accordingly.

Key findings

- Only 70% of organizations fully met Requirement 6 at interim assessment.
- Requirement 6 has proved to be one of the most challenging Key Requirements ever since the inception of PCI DSS more than a decade ago.
- Control 6.6 (Protect public-facing web applications against known attacks) made its entrance into the "Bottom 20" list of non-compliant controls.
- Organizations had the most difficulty with controls 6.2 (Protect components and software from known vulnerabilities) and 6.6 (Protect public-facing web applications against known attacks).
- Controls 6.3 (Develop internal and external software applications securely) and 6.4.5 (Change control procedures for security patches) entered the top 20 compliant controls for North America.
- Control 6.2 is now on the "Bottom 20" list in Asia-Pacific.
- Requirement 6 ranks low on the use of compensating controls. Between 2012 and 2014, 30% of organizations used compensating controls; in 2015, just 6% of organizations did so.
- Service providers (94.6% average compliance) slightly outperformed merchants (92.2% average compliance) on Requirement 6.

Proportion of companies fully compliant

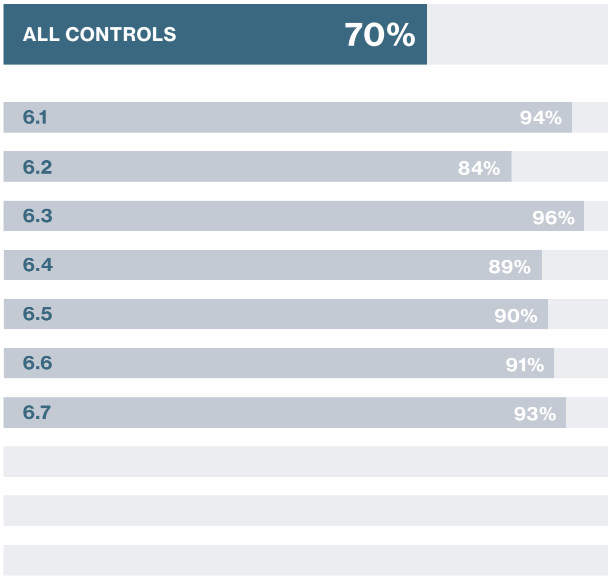


FIG 29 – Requirement 6: % organizations fully compliant

Average control gap

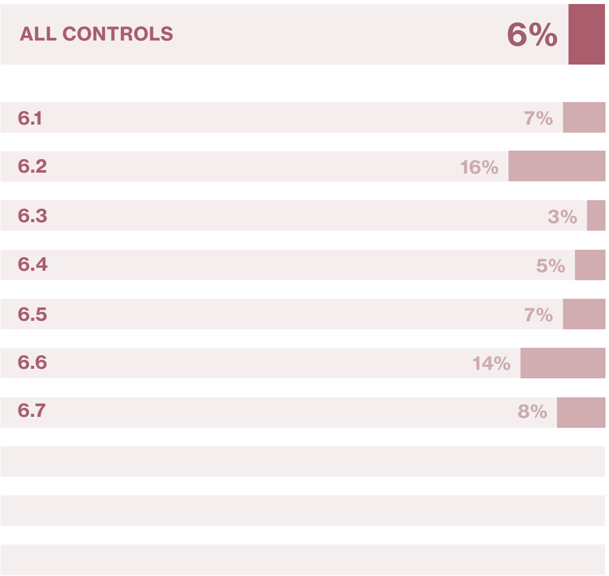


FIG 30 – Requirement 6: average % of controls not in place

★ **All industries** 70%

Retail and hospitality 67%

Average compliance with Requirement 6 across retail and hospitality was 93.1% – a control gap of 6.9%. But full compliance at the interim assessment was 67%. This suggests that there were some issues with Requirement 6 across all retail and hospitality organizations.

Control 6.6 had the lowest average compliance – with a control gap of 25%. Web applications should already be included in all internal and external vulnerability scans, and annual penetration tests. But this requirement mandates either the implementation of a web application firewall, or an independent vulnerability assessment of web applications after "any change" – not, as in many other places in the PCI DSS, only after "any significant change".

Financial services 67%

The control gap in financial services was 7.6%. It performed best on control 6.3 – with a control gap of just 1.1%, this is one of the most compliant controls within financial services. The challenge is with control 6.6, where the control gap was 13.3%.

IT services 92%

The IT services industry had good average performance, with a very low control gap of just 1.1%. And IT services performed relatively well at interim assessment, achieving full compliance with all controls except 6.5 (Address common coding vulnerabilities) – this was met by 92% of organizations.

Base control 6.5 has 13 sub-requirements, which include strenuous technical testing of all code and applications that interact with cardholder data. Manual testing can be time-consuming, while automated testing can be costly. The key is finding a good balance of the two methods, and training developers in secure code review so that the process is not hindered or incorrect.

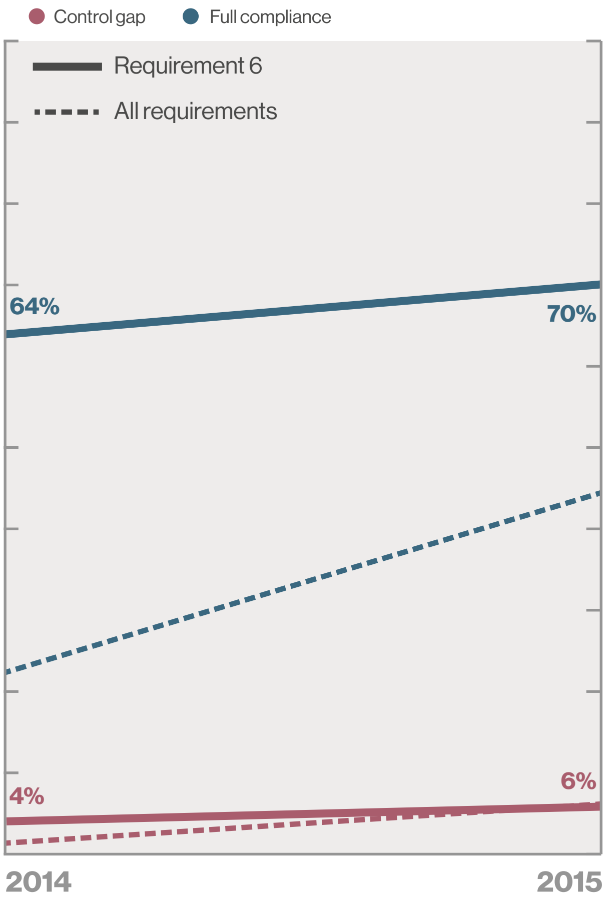
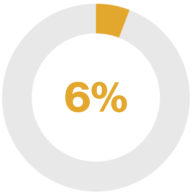


FIG 31 – Requirement 6: 2014 – 2015 comparison

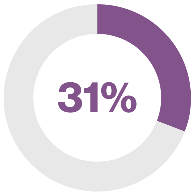
Year-over-year comparison

While performance improved, organizations continued to struggle with Requirement 6. There was a significant decline of 7.6 percentage points in the average proportion of controls in place for control 6.6.

Organizations have improved maintenance, with controls concerning secure code development, change control and patching. A concerted effort is still needed to establish a process and identify security vulnerabilities (6.1), and to protect public-facing web applications (6.6) against these new threats. These processes must be communicated to those affected across the entire organization (6.7).



6% of organizations used one or more compensating controls for Requirement 6 in 2015, down from 30% in 2014.



31% had Requirement 6 in place at the time of a breach—up from 0% in 2014.

Key Requirement 7:
Restrict access

Requirement 7 specifies the processes and controls that should be in place to restrict each user's access rights to the minimum they need to perform their duties – a "need to know" basis.

Our 2015 report mentioned that Requirement 7 scored the highest on sustainability. It has no frequent compliance tasks explicitly specified within the DSS (similar to Requirement 2). It is usually highly automated and requires less frequent attention compared to other requirements. It also has the least amount of changes in previous updates to the standard.

Key findings

- 87.1% of organizations met all Requirements at their interim assessment, demonstrating that they remain compliant all year round.
- Requirement 7 ranked second in terms of full compliance out of the 12 Key Requirements – it was first in 2014.
- Organizations in Europe slightly outperformed other regions for this Requirement.
- Controls 7.2 (Access control system based on need to know, set to deny all) and 7.3 (Policies and procedures for restricting access to CHD) achieved 100% compliance in the North America region.
- None of the Requirement 7 controls appeared in the 2014 "Bottom 20". But in 2015, control 7.1 (Limit access to system components) entered the list at the number 20 spot.
- As in 2014, no organizations in our data set applied compensating controls to any of the controls under Requirement 7.

Proportion of companies fully compliant

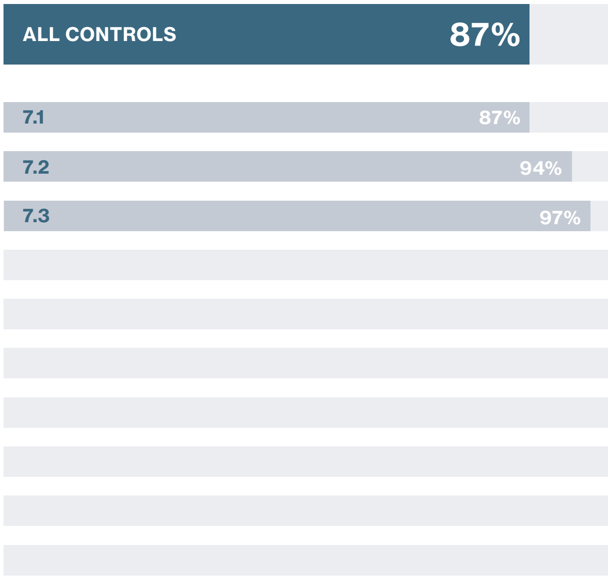


FIG 32 – Requirement 7: % organizations fully compliant

Average control gap

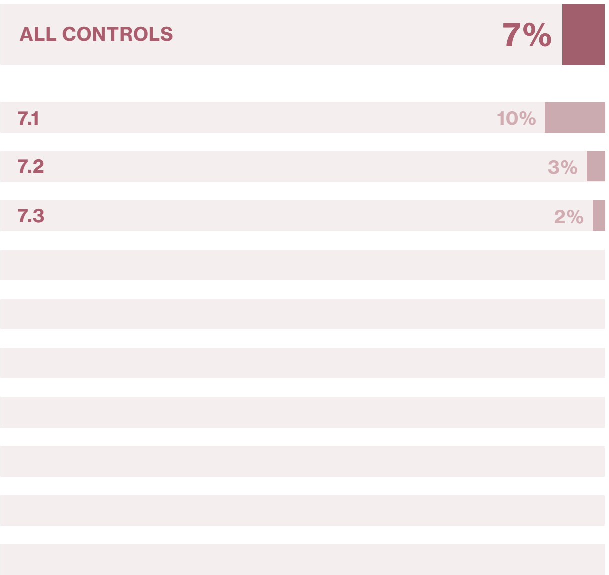
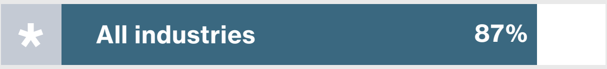
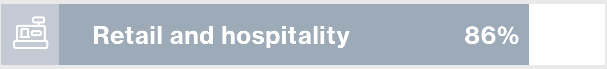


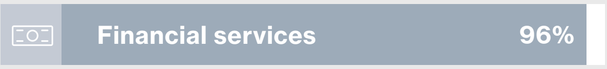
FIG 33 – Requirement 7: average % of controls not in place



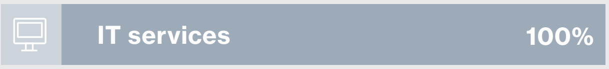


The control gap for Requirement 7 in retail and hospitality was 7.3%. Average compliance was high against controls 7.2 and 7.3.

But there was a control gap of 10.8% for control 7.1; 14% of organizations failed to achieve this control at interim assessment. While many companies have strong access control systems in place, these can weaken somewhat as they're stretched to more locations outside of the corporate headquarters. Ensuring that satellite locations are following domain policies can sometimes prove difficult.



The control gap in financial services was just 0.5%. Performance against control 7.1 (1% control gap) stopped it from achieving a perfect score. Most financial services organizations have a robust and secure access control mechanism in place. But they are not often configured specifically for PCI DSS compliance, and assessments can discover some necessary tweaks.



The IT services industry achieved 100% compliance. Organizations generally demonstrate proficiency in their ability to assign and manage access permissions. Organizations benefit from use of updated technology, where the latest systems and applications generally come out preconfigured in a compliant and secure manner. Some technologies even have built-in PCI DSS audits, or modules, simplifying the effort and workload. Hence, access control mechanisms seem to be one of the first things in place.

In addition, having a comparatively smaller pool of employees with access to CHD, or responsibility for the security of the CDE, makes role-based access control (RBAC) easier to implement for IT services organizations.

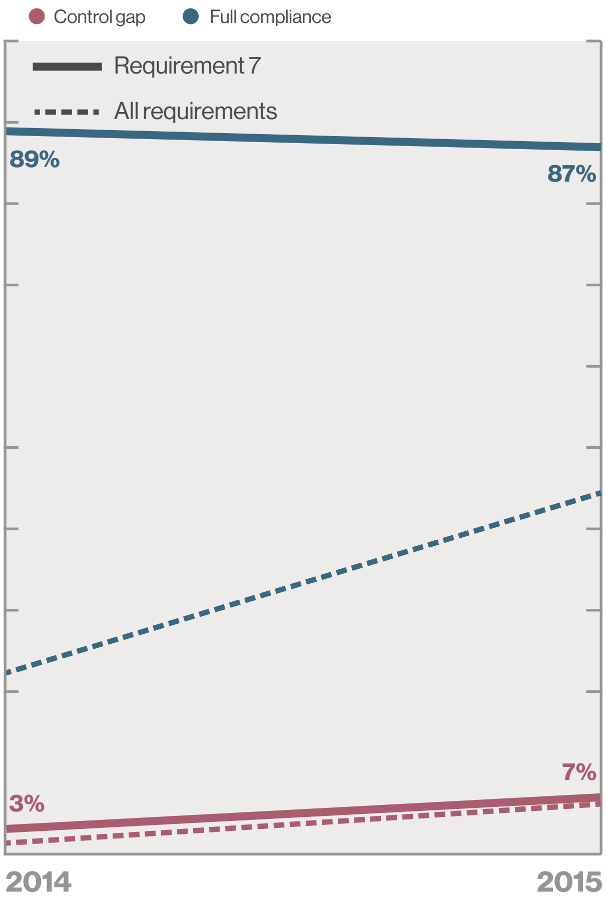
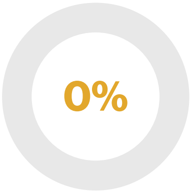


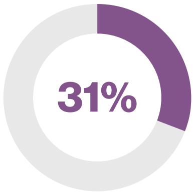
FIG 34 – Requirement 7: 2014 – 2015 comparison

Year-over-year comparison

Looking at average compliance since 2008 shows Requirement 7 is not proving a major difficulty for most organizations. While compliance fell slightly in 2015 (both full compliance at interim assessment and average compliance), performance against Requirement 7 is still better than against most other Key Requirements.



Again in 2015, no companies used a compensating control for Requirement 7.



31% had Requirement 7 in place at the time of a breach—up from 27% in 2014.

Key Requirement 8:
Authenticate access

Requirement 8 sets standards for managing user identities and authentication methods, including passwords. Prior to PCI DSS 3.x, the description for the Requirement was “Assign a unique ID to each person with computer access”. This has changed to “Identify and authenticate access to system components” – a more complete description of the controls within the requirement.

Key findings

- 81% of organizations met all requirements at interim assessment in 2015.
- The proportion of companies fully compliant at interim assessment increased by 12.5 percentage points year-over-year. The control gap was static.
- As in 2014, organizations struggled most with control 8.2 (Ensure proper user authentication management on all system components), although performance did improve year-over-year.
- Organizations in Europe experienced more difficulty with Requirement 8 than those in North America or Asia-Pacific.
- The most challenging testing procedure in North America was 8.2.3.a (Verify that user password parameters are set to require a minimum strength/complexity).
- Controls 8.1 (Policies and procedures for user identification) and 8.5 (Do not use group, shared IDs) had the biggest control gap in Europe.
- Requirement 8 remains the Key Requirement for which the greatest proportion of compensating controls are used – particularly in Asia-Pacific.
- North American organizations applied compensating controls mainly to controls 8.2 and 8.5 (Do not use group, shared IDs).

Proportion of companies fully compliant

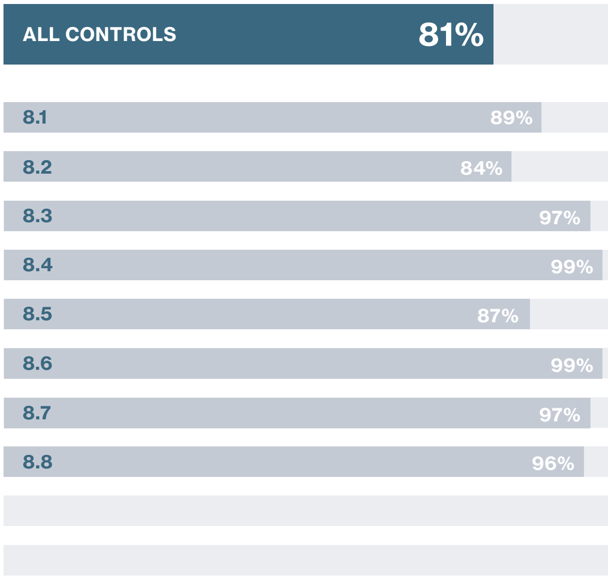


FIG 35 – Requirement 8: % organizations fully compliant

Average control gap

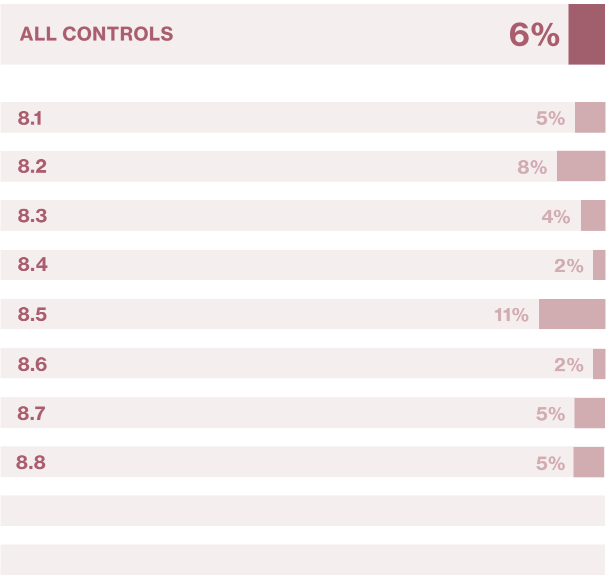
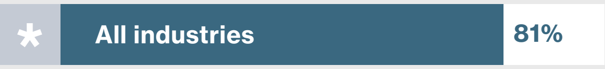
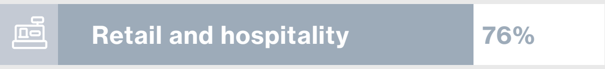
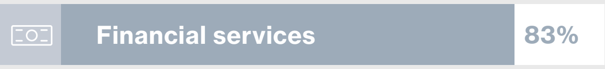


FIG 36 – Requirement 8: average % of controls not in place



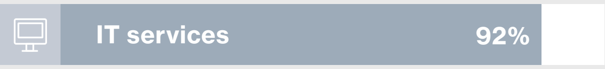


An average of 8.3% of Requirement 8 controls were found not to be in place in retail and hospitality. Requirement 8.5 proved to be the biggest hurdle, with a control gap of 21%. The hospitality industry has the biggest issue with the use of groups and shared IDs. It's a case of putting convenience and speed before compliance. It's a quick workaround in an industry where employees sometimes fail to show up without notice and the workforce can change each season.



The financial services industry recorded a control gap of just 3.4% – its third-best performance across the 12 Key Requirements. It achieved 100% compliance with half of the controls. Those needing attention are: 8.8 (Policies and procedures for identification and authentication) and to a lesser extent 8.1, 8.2 and 8.5.

It's possible organizations have had systems in place for some time that are functioning and compliant. But they're difficult to assess if they aren't documented. Performing regular security assessments helps ensure there's a continuous focus on the overall security and compliance posture of an organization.



The IT services industry outperformed all other industries on Requirement 8, with a control gap of just 0.7%. It achieved full compliance with all of the eight base controls except 8.1 (control gap, 1.6%) and 8.2 (0.7%). Proper documentation and management of user authentication is the next maturity level for IT services to achieve. The industry does meet the requirements for accurate implementation.

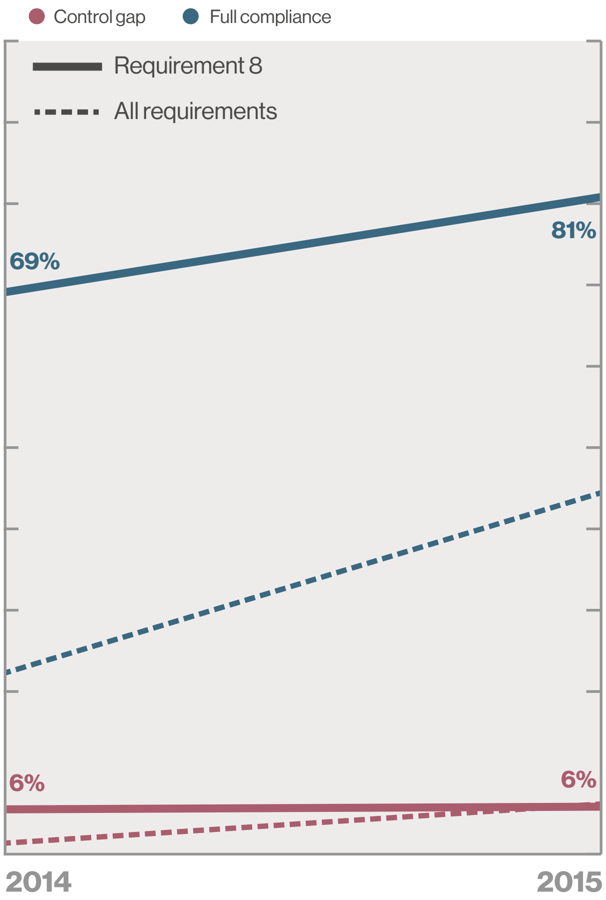
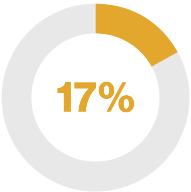


FIG 37 – Requirement 8: 2014 – 2015 comparison

Year-over-year comparison

There was a year-over-year improvement of 12.5 percentage points in the proportion of organizations that met all requirements at interim assessment. The control gap remained static. While Requirement 8 again saw the greatest use of compensating controls, their use fell significantly.



17% of organizations used one or more compensating controls for Requirement 8 in 2015, down from 67% in 2014.

50% had Requirement 8 in place at the time of a breach—up from 27% in 2014.

Key Requirement 9:
Control physical access

Requirement 9 aims to restrict and monitor physical access to equipment or sensitive locations. Physical security measures combine administrative procedures (e.g. escorting visitors) and physical deployments (e.g. badge access readers) to control access based on personnel classification (e.g. employees, contractors, visitors).

Attackers have proven adept at defeating logical access controls when they gain unfettered or unmonitored physical access to media or devices (e.g. laptops, POS kiosks etc.). POS terminals, gas pumps and ATMs are in attackers' crosshairs whenever physical security controls are inadequate.

Key findings

- 81% of organizations achieved full compliance at their interim assessments.
- Control 9.9.3 (Training for personnel, be aware of tampering) is amongst the least compliant controls in the European region; average compliance with this control was 100% in the Asia-Pacific region.
- Very few organizations (3%) in our data set applied compensating controls to any of the controls under Requirement 9.
- Service providers saw their best performance across all 12 Key Requirements in Requirement 9. They achieved a control gap of 1.7%.

Proportion of companies fully compliant

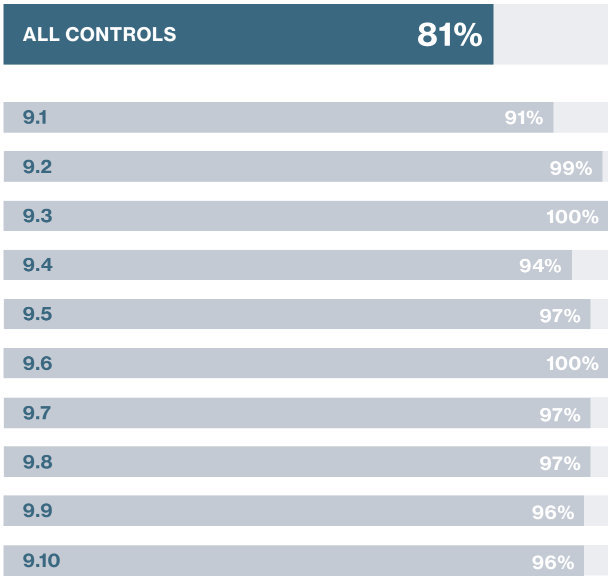


FIG 38 – Requirement 9: % organizations fully compliant

Average control gap

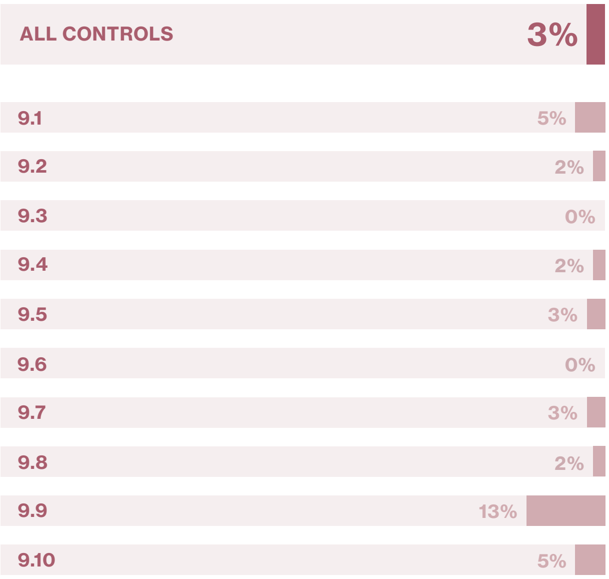


FIG 39 – Requirement 9: average % of controls not in place

All industries 81%

Retail and hospitality 71%

The compliance gap in retail and hospitality was 6%. Full compliance was achieved for controls 9.2, 9.3 and 9.6. But 29% of organizations failed to meet all Requirements at their interim assessment. And the biggest challenge was posed by control 9.9 (Protect data capture devices; tampering/substitution), where there was a control gap of 12.5%.

All testing procedures under base control 9.9 have caused some issues as they were only recently introduced. Retail organizations prepared better for the changes than those in hospitality. High-profile breaches in retail have seen security rise up the business agenda. In hospitality, POS devices sometimes belong to vendors and sometimes to franchisees. Establishing ownership of the devices has likely held up compliance with 9.9.

Financial services 75%

The financial services industry achieved a high level of compliance on Requirement 9, with a control gap of just 1.6%. This was the second-highest performing Key Requirement for this industry. Most base controls under Requirement 9 (controls 9.3, 9.5, 9.6, 9.8, 9.9) achieved 100% compliance.

The poorest performance came in control 9.1 (Appropriate facility entry controls and monitoring access of CDE), with a control gap of 10.1%. A lot of companies rely on third-party facilities for the hosting and physical management of their technology. Some of these companies may not meet PCI DSS requirements, which is why it's critical to include any third-party locations in the annual assessment.

IT services 100%

The IT services industry achieved full compliance with all controls in Requirement 9.

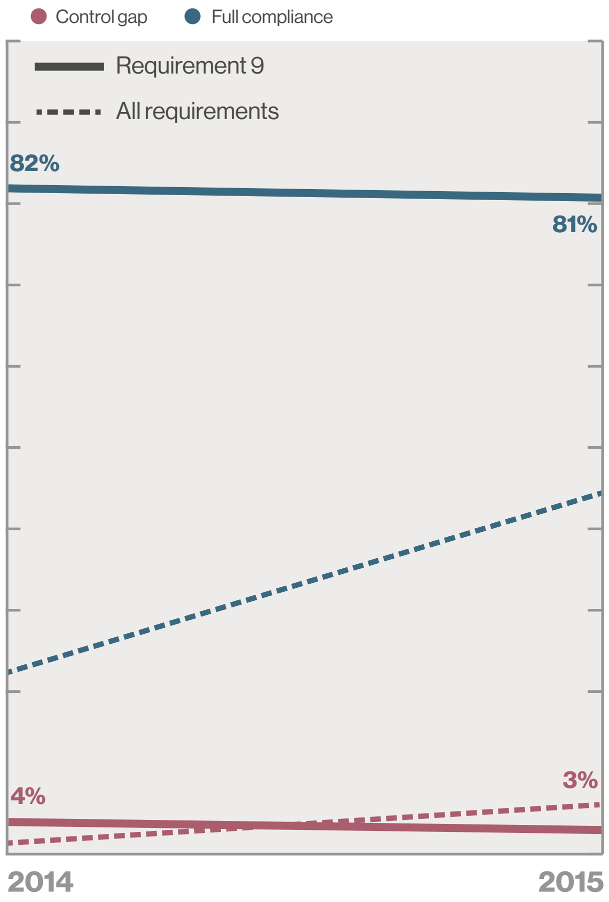
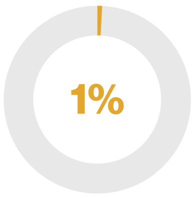


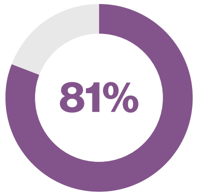
FIG 40 – Requirement 9: 2014 – 2015 comparison

Year-over-year comparison

Looking at the overall figures, compliance with Requirement 9 remained fairly static.



1% of organizations used one or more compensating controls for Requirement 9 in 2015, down from 3% in 2014.



81% had Requirement 9 in place at the time of a breach—down from 82% in 2014.

Key Requirement 10: Track and monitor access to networks and cardholder data

While many of the PCI DSS Requirements aim to deter or prevent an attack, Requirement 10 sets standards around the detection of issues. Attacks happen; deterrent and preventative controls do fail. Having detective controls that can identify the source, nature, timing, and even exfiltration destination of a breach can prove critical to limiting the potential damage of a breach and putting corrective measures in place as quickly as possible.

Requirement 10 is intended to serve as an enabler of rapid incident response, effective business continuity and disaster recovery. Post-recovery, Requirement 10 is also designed to provide the data needed to determine the timeline of malicious events, and strengthen preventative and deterrent controls.

Key findings

- In our interim assessments, 80% of organizations fully met Requirement 10 and maintained year-round compliance.
- Average compliance declined year-over-year across all controls under Requirement 10 except 10.1 (Ensure audit trails link access to individual users), where it improved by 2.2 percentage points.
- Requirements 10.2 (Implement automated audit trails) and 10.5 (Secure audit trails so they cannot be altered) saw the greatest use of compensating controls under Requirement 10.
- Requirement 10.4 (Time-synchronization technology) was in the "Bottom 20" of non-compliant controls in North America.
- Service providers (92.9%) scored slightly ahead of merchants (91.1%) for average compliance with Requirement 10.

Proportion of companies fully compliant

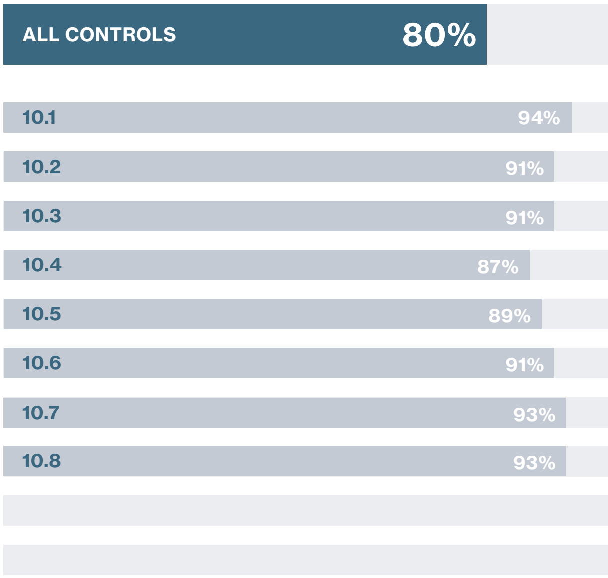


FIG 41 – Requirement 10: % organizations fully compliant

Average control gap

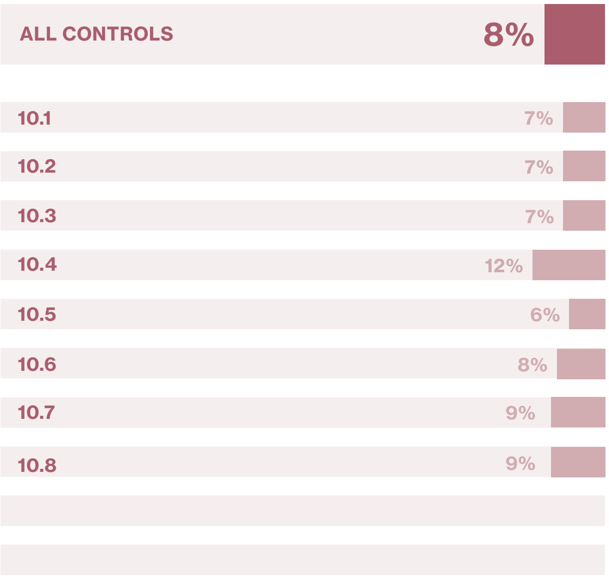


FIG 42 – Requirement 10: average % of controls not in place

★	**All industries**	80%
	Retail and hospitality	71%

The average control gap in retail and hospitality for Requirement 10 was 6.9%. Retail and hospitality organizations encountered most difficulty at their interim assessments with base control 10.5, with 76% achieving full compliance. In terms of average performance, control 10.7 (Retain audit trail history for at least a year) proved the most challenging – although this was an issue in hospitality, not retail.

	Financial services	83%

The financial services industry was outperformed by all other industries for Requirement 10 in terms of average compliance, with a control gap of 11.8%. Financial services organizations had most success with control 10.1 – 96% met the requirements at interim review. They struggled, however, with 10.8 (Ensure policies and procedures for monitoring access are in use) – 88% were fully compliant; the control gap was 18.7%. This is a common issue – failing to document procedures that were often themselves compliant.

	IT services	83%

Just 2% of controls on average were not in place in the IT services industry. It was fully compliant with controls 10.2, 10.3 (Record minimum audit trail entries), 10.5, 10.7 and 10.8. The least successful controls were 10.1 and 10.4.

Configuring audit systems to match PCI DSS requirements is a constant struggle. Most solutions are not compliant out of the box and will require some adjustments. Time synchronization is generally solid when it comes to the corporate headquarters, but where it rests with satellite locations, the corporate domain controller or other central timeserver sometimes has little oversight.

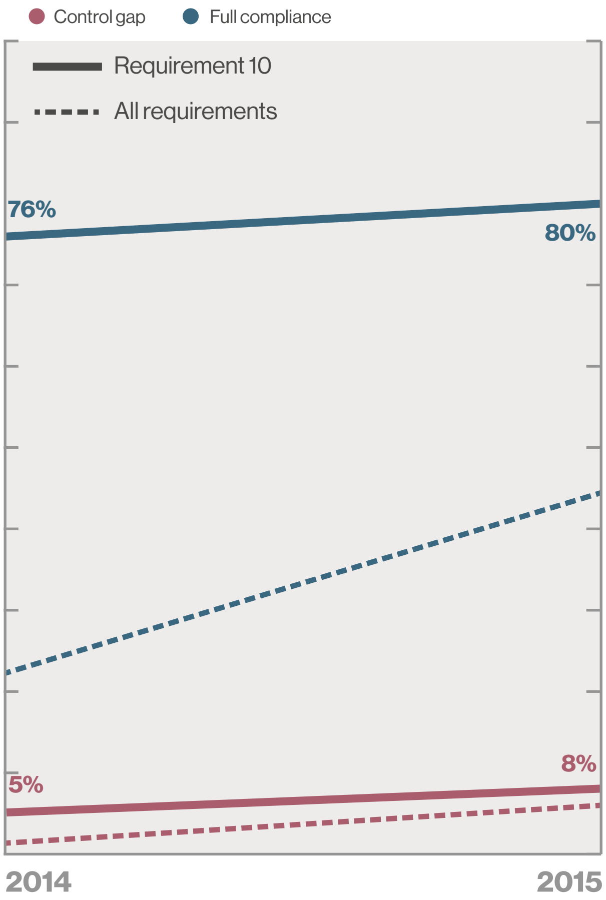
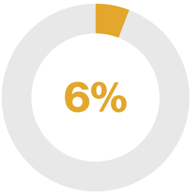


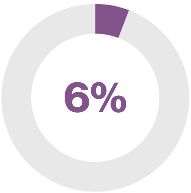
FIG 43 – Requirement 10: 2014 – 2015 comparison

Year-over-year comparison

The proportion of organizations meeting all requirements at interim assessment increased by 4.4 percentage points year-over-year. However, the control gap widened.



6% of organizations used one or more compensating controls for Requirement 10 in 2015, down from 12% in 2014.



6% had Requirement 10 in place at the time of a breach—up from 0% in 2014.

Key Requirement 11:
Test security systems and processes

Requirement 11 focuses on organizations' abilities to identify and respond to vulnerabilities before attackers exploit them. That's vital because network environments are constantly changing as new assets are introduced and flaws are identified in existing ones – and attacks are becoming more sophisticated and automated on a global scale.

The controls cover the periodic use of sensors and scanners to gauge how susceptible organizations are to compromise attempts, based on mimicry of attackers' behavior. The controls range from detecting unauthorized wireless access points to evaluating the effectiveness of network barrier enforcements.

Key findings

- 70% of organizations demonstrated that they had maintained all Requirement 11 controls all year. That was a big improvement on 2014's 33%.
- As in 2014, four of the Requirement 11 controls were in the "Bottom 20".
- Again, 11.2 (Run network vulnerability scans) is the one with the lowest compliance. Executing the vulnerability scans isn't the problem. The main issues were with 11.2.3.b (Review scan reports and verify that the scan process includes rescans) and 11.2.1.b (Review the scan reports and verify that the scan process includes rescans until all "high-risk" vulnerabilities addressed).
- Both merchants and service providers performed poorly on Requirement 11.

Note: changes to this requirement introduced in PCI DSS 3.2 will impact results next year. For example, "within the cardholder data environment" was removed from test procedure 11.5, which will impact organizations that do not carry out change detection on all in-scope systems.

Proportion of companies fully compliant

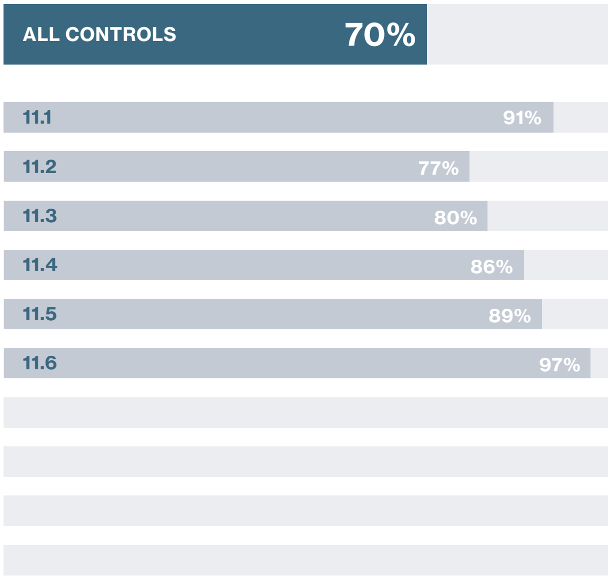


FIG 44 – Requirement 11: % organizations fully compliant

Average control gap

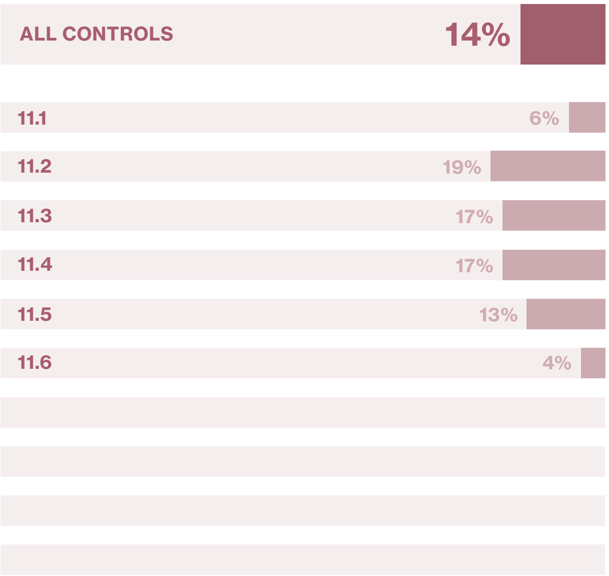


FIG 45 – Requirement 11: average % of controls not in place

All industries 70%

Retail and hospitality 57%

Requirement 11 saw the lowest average compliance in retail and hospitality, where the control gap was 18.8%. And only 57% of organizations were fully compliant at their interim assessments. Full compliance was achieved on control 11.6 (Documented procedures for monitoring and testing). But controls 11.2 (control gap, 27.3%) and 11.4 (Use intrusion-detection systems – 24.1%) proved particularly challenging.

Vulnerability scanning solutions (11.2) are both expensive and resource intensive, and free versions typically require heavy customization. Once the scanner is set up there can be little oversight of when a scan completes. Don't assume that the scan will automatically take care of any identified issues; there needs to be human involvement. For organizations with many locations, central processes and solutions might mean scans are executed regularly, but follow-up and remediation efforts depend on remote resources – and these might not be as well-trained.

Financial services 79%

15% of controls weren't in place on average in financial services. The worst performance was on control 11.4, with a control gap of 26.7%. Intrusion-detection systems are both costly and resource intensive (if not completely automated), so many companies will either not purchase them, or do not know that they are required for PCI compliance.

IT services 83%

The IT services industry outperformed all other industries, with a near-perfect average – the control gap was just 0.7%. Average compliance was 100% on all requirements except 11.3 (Implementation of penetration testing) – although this still recorded a control gap of just 3%.

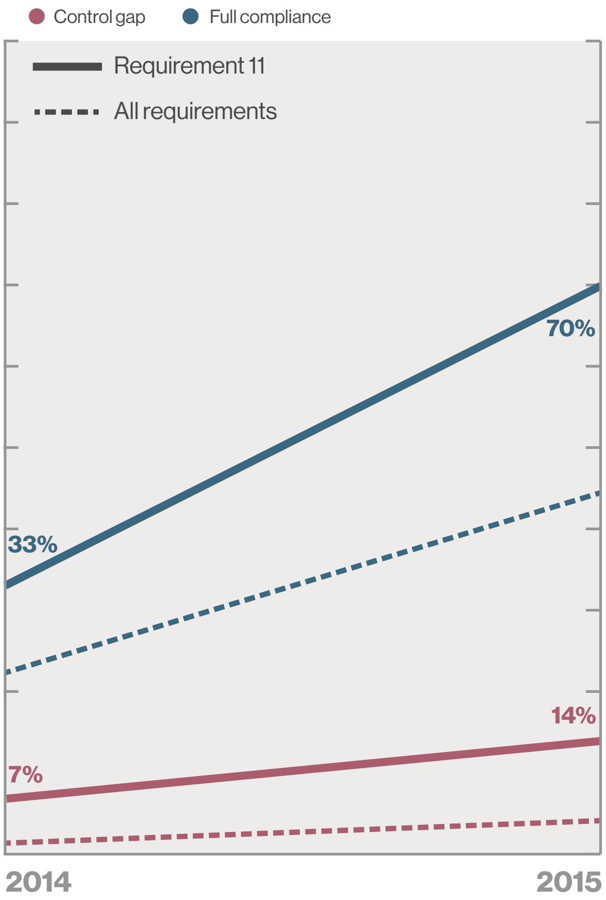
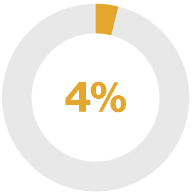


FIG 46 – Requirement 11: 2014 – 2015 comparison

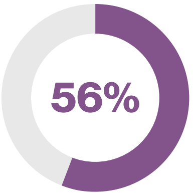
Year-over-year comparison

In full compliance at interim assessment, there was a huge year-over-year improvement of 36.7 percentage points. Average compliance also improved slightly by 2.6 percentage points. This was largely due to a significant improvement of 12 percentage points on control 11.3.

But Requirement 11 remains one of the Key Requirements that organizations struggle with the most. And average compliance with control 11.4 declined by 12.4 percentage points.



4% of organizations used one or more compensating controls for Requirement 11 in 2015, down from 14% in 2014.



56% had Requirement 11 in place at the time of a breach—up from 9% in 2014.

Key Requirement 12:
Maintain an information security policy

For controls to be effective, they can't exist in isolation. They need to be part of a system of connected and coherent controls. Since the start of PCI DSS 3.x, requirements for well-documented, distributed policies and procedures that are understood by relevant personnel have been distributed throughout the standard. The last control of each requirement expects organizations to maintain relevant policies and procedures.

Requirement 12 takes this a step further by calling for clear communication and frequent reinforcement of an organization's goals for data protection and compliance. It also requires the development of an overarching security policy that ties all the policy requirements of previous controls into a single security policy framework. It might feel at first like a mix of leftover security topics, but it actually provides another layer in the administration of a control system and adds further requirements – for example, covering incident response and third-party management.

Key findings

- 70% of organizations fully met Requirement 12, making it the lowest ranking Key Requirement alongside 1, 6 and 11.
- Most controls saw year-over-year improvements, but there was an 18.5 percentage point decline in average compliance in control 12.9 (Service provider security responsibility). This new control was introduced in PCI DSS 3.0.
- Controls 12.2 (Risk assessments), 12.8 (Managing service providers with whom CHD is shared or that could affect the security of cardholder data) and 12.9 all appeared in the "Bottom 20" controls in the North America region. Europe's "Bottom 20" included controls 12.8, 12.9 and 12.10. These controls did not appear in Asia-Pacific's "Bottom 20".

Proportion of companies fully compliant

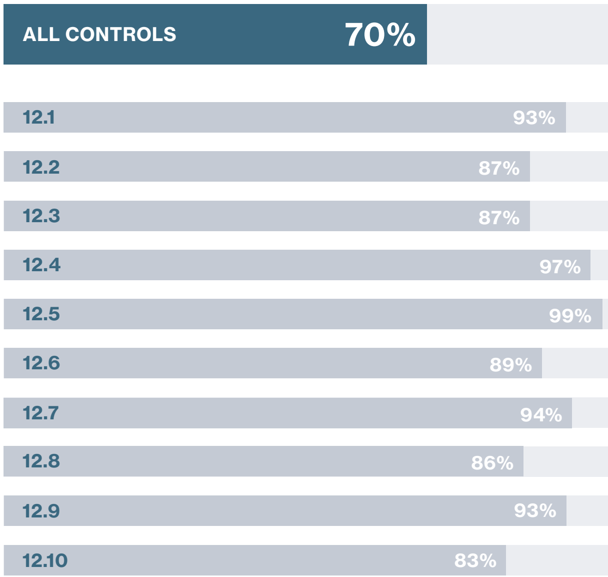


FIG 47 – Requirement 12: % organizations fully compliant

Average control gap

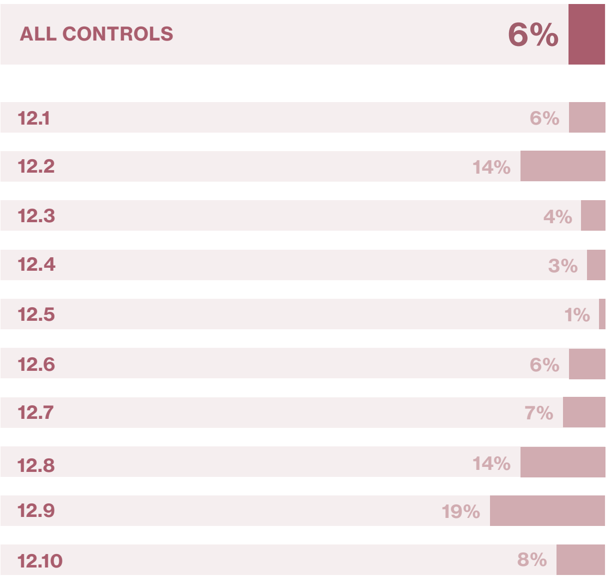


FIG 48 – Requirement 12: average % of controls not in place

All industries 70%

Retail and hospitality 62%

Over a third of retail and hospitality organizations failed to achieve full compliance with Requirement 12. The control gap was 7.6%. Poorest performance was in 12.9, where the control gap was 33.3%, and 12.8 (control gap of 12.1%). Organizations had the biggest problem with 12.8 when choosing service providers that were not PCI DSS compliant. In these instances, the service providers are often unprepared to be included in the organization's assessment and demonstrate PCI-compliant controls of their own.

Financial services 63%

The financial services industry achieved full compliance with control 12.5 (Formally assign information security responsibilities). But it fared less well with other controls. On average, 44.4% of companies did not have control 12.9 in place. The industry also struggled with 12.2 (compliance gap of 26.5%) and 12.8 (21.3%).

Service provider agreements can get confusing and many customers do not have adequate legal representation to quickly confirm that the correct agreements are in place as needed for control 12.8. The core of control 12.9 is that a service provider acknowledges that while any cardholder data is in its network, it is responsible for it.

IT services 92%

In contrast with the other sectors, the control gap for IT services was just 2.6%. It achieved full compliance with controls 12.1, 12.4, 12.5, 12.6, 12.7, 12.9 and 12.10. The least successful controls were Requirements 12.2, 12.8 and 12.3 (Develop usage policies for critical technologies).

When it comes to risk assessments, the issue is often a lack of training. Most companies will point customers to something like the NIST SP 800 series of documentation but not give actual training or guidance on how to carry out a compliant risk assessment.

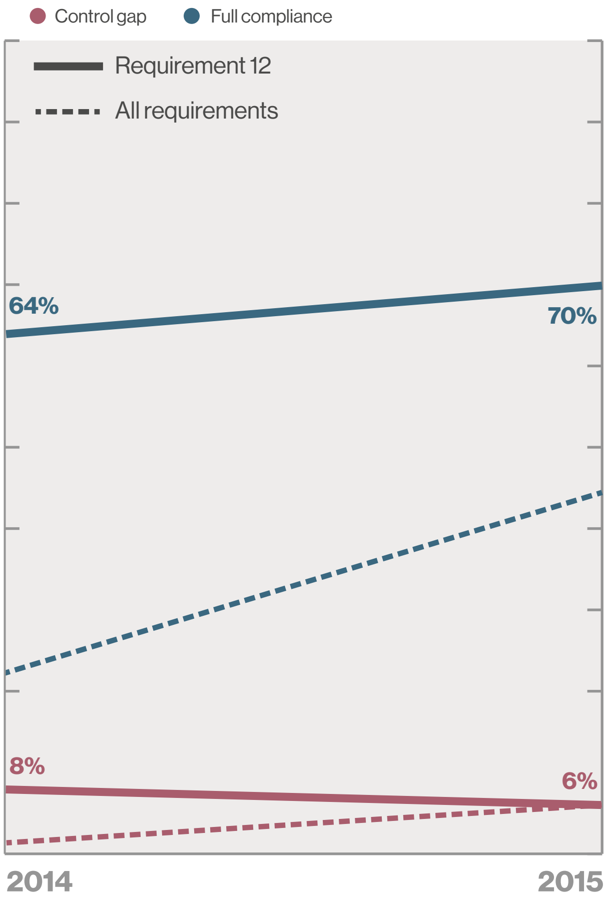
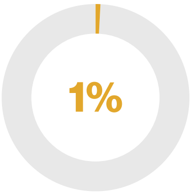


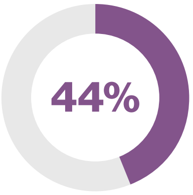
FIG 49 – Requirement 12: 2014 – 2015 comparison

Year-over-year comparison

Compliance in 2015 was up on 2014, both in terms of full compliance at interim assessment and average compliance. But organizations still struggle with many of the controls under Requirement 12.



1% of organizations used one or more compensating controls for Requirement 12 in 2015, down from 3% in 2014.



44% had Requirement 12 in place at the time of a breach—up from 9% in 2014.

Appendix A:
Bottom 20 lists

Some old favorites. like control 11.2 (Run network vulnerability scans) and 10.4 (Time-synchronization technology) appear in the Bottom 20 of least compliant controls again this year. It is also disappointing to see that organizations are failing on password requirements (8.5 and 2.1.1.b).

It is noticeable that penetration testing and scanning appear frequently in the Bottom 20 for both controls and testing procedures. The biggest outlier is 4.1.1, with 40% failing at interim assessment – no doubt due to tighter restrictions on permissible versions of TLS and the phase-out of all SSL versions.

Bottom 20 base controls by full compliance

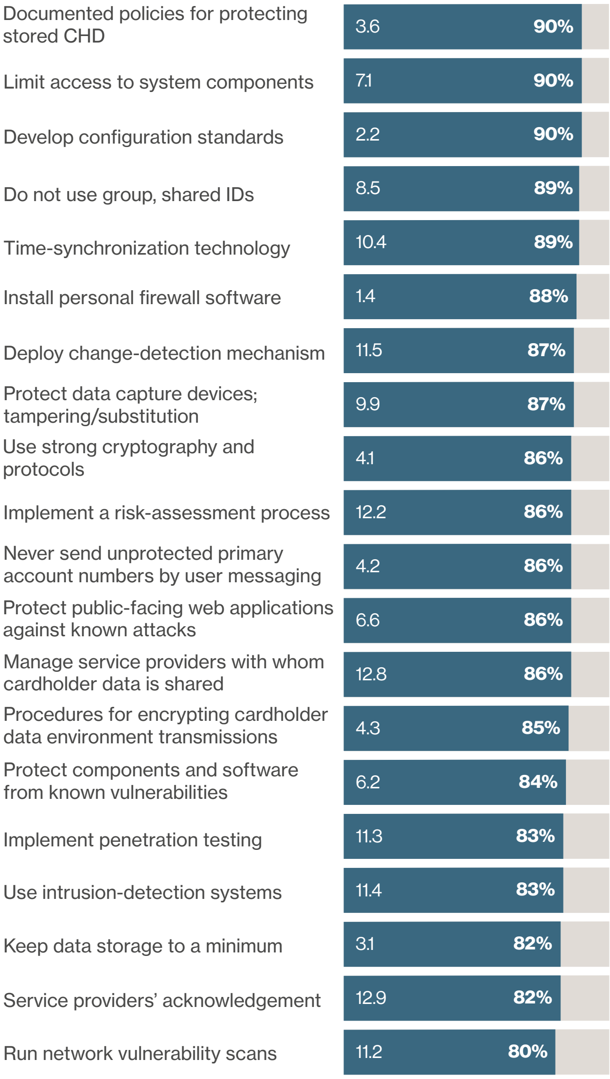


FIG 50 – Bottom 20 base controls by full compliance

Bottom 20 testing procedures by control gap

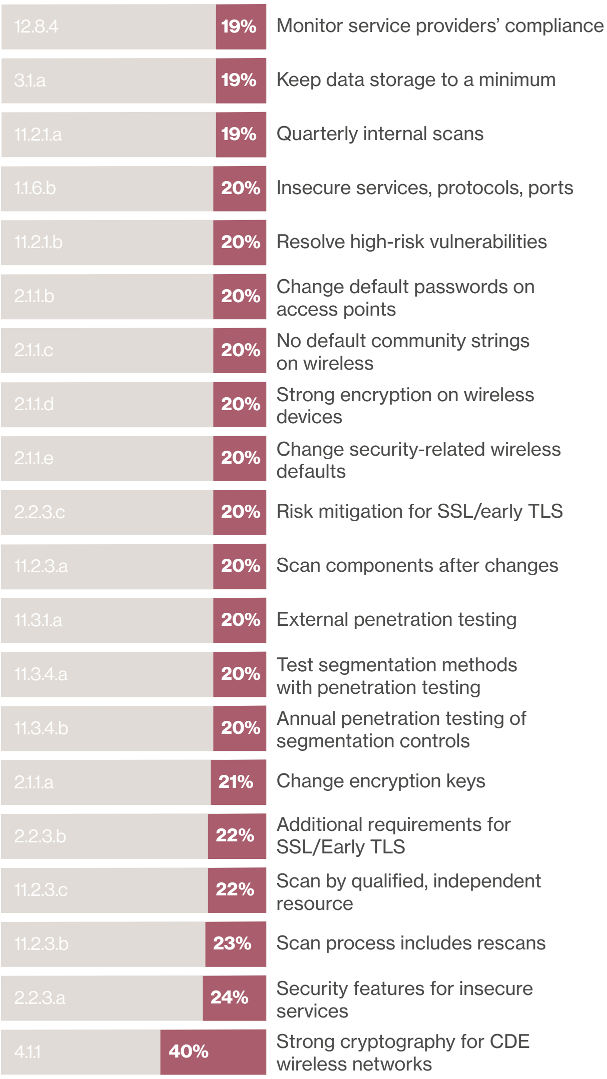


FIG 51 – Bottom 20 testing procedures by control gap

Appendix B:
The lifecycle of PCI DSS controls

Lack of understanding of the control lifecycle is a contributory factor in degrading control environments, which can ultimately result in security breaches and data compromises. It's essential that organizations understand how each stage of the control lifecycle can influence the underlying supporting processes, overall operational efficiency and effectiveness of security controls.

1. Conception

During the first stage of the control lifecycle, the need for, or applicability of, a control is identified, followed by systematic exploration of the control criteria, its functional specifications and the available options. This is essential to determine its suitability as a safeguard to avoid, detect, minimize and counteract risks.

2. Design and build

The design and build stage determines, defines and documents the exact purpose and functional parameters of each control. Since each control environment is unique to an organization, it's important to determine the applicability and suitability of each PCI DSS Requirement. This control profile should include the relationship between the control and the risks it's intended to mitigate.

The security control lifecycle

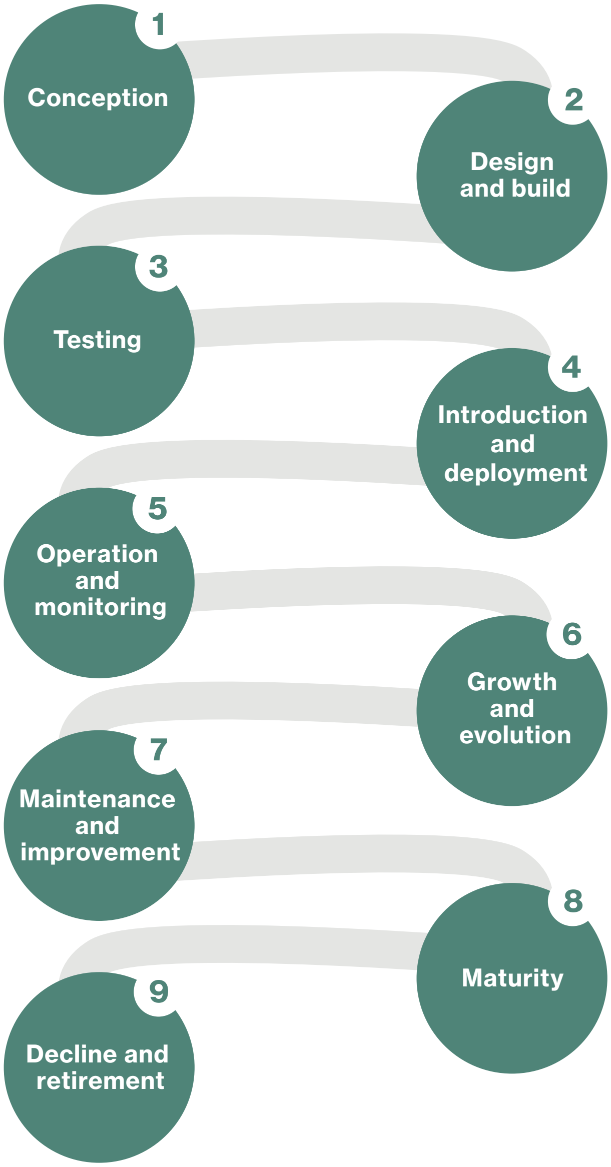


FIG 52 – Control lifecycle

Without continuous monitoring, maintenance and improvement, the effectiveness of the control will eventually shrink.

3. Testing

The control testing stage determines the extent to which a control follows prescribed specifications in actual practice. It's the best opportunity to determine how the control may impact people, systems, procedures and third parties prior to deployment, and what the supporting requirements are for the control to operate in a sustainable manner.

4. Introduction and deployment

This stage marks the initial introduction or broader deployment of the control after benchmarking performance within a test environment. This is one of the most critical stages in the lifecycle. The manner in which new security controls are introduced can have immediate and long-term consequences on success or failure – particularly affecting the way controls are perceived and accepted by people and systems within the organization. New controls seldom perform flawlessly from the start and, depending on the amount of testing before deployment, may require an amount of tailoring during and after deployment to iron out shortcomings in their operation, maintenance and support performance.

5. Operation and monitoring

This stage involves keeping the control under systematic review, by observing, collecting, storing and reporting state and performance data over time, and supervising control activities to determine if control objectives and performance targets are being met.

6. Growth and evolution

It is common for a control to evolve in response to its environment. The growth and evolution stage is typically characterized by changes to the control to enhance and refine its functions and operation by augmenting configurations in IT systems, updating documentation, improving processes etc.

7. Maintenance and improvement

The organization monitors control behavior and performance, and evaluates how changes in the control environment impact the control. In dynamic compliance environments, there is always a need to perform routine actions – either corrective, planned, predictive, preventative or adaptive control maintenance – to keep the control operating according to standards or specification. The organization also needs to consider and apply any control modifications or improvements to strengthen the organization's security posture, advance the desirable qualities of a control and improve its operation, efficiency and effectiveness.

8. Maturity

During the maturity stage, the control is established, and has a track record of performance meeting all operational requirements. The control should have a reasonable level of robustness (ability to resist unwanted change) and resilience (ability to recover from unwanted change). The organization now aims to maintain the optimized control environment that has been created.

9. Decline and retirement

The final stage is the replacement or termination of a security control from an operational environment when it has reached the end of its useful function or is being replaced by a more effective or efficient control. This transition is known as the decline stage of the control lifecycle. Shrinkage in effectiveness could be due to changes in the control environment or external changes. Sometimes the decline occurs rapidly, making it evident and easily detectable. In many cases it happens gradually, over time, and the decline in control effectiveness is noticed only when a security breach is detected.

Appendix C:
Compliance calendar

REQ.	AREA	DSS 3.2	ACTIVITY	IMMEDIATELY	DAILY	WEEKLY	MONTHS	ANNUALLY	PERIODICALLY	AFTER CHANGES
	Scope management	ALL	Confirm locations and flows of CHD, and ensure inclusion in the PCI DSS scope.					✓		
1	Firewalls and routers	1.1.7	Review firewall and router rulesets.				6			
3	Data retention	3.1.b	Identify and delete stored CHD that has exceeded defined data retention periods.				3			
	Cryptographic keys	3.6.4	Change cryptographic keys that have reached the end of their cryptoperiod.						✓	
6	Patch management	6.2	Install all critical security patches within one month of release.				1			
	Patch management	6.2	Install all non-critical security patches (recommended).				3			
	Software development	6.5	Train developers in latest coding techniques. ★					✓		
	Public-facing web applications	6.6	Assess vulnerability of public-facing web apps. N/A if you use a Web App Firewall.					✓		✓
8	User access management	8.1.3	Revoke access for terminated users.	✓						
	User access management	8.1.4	Remove/disable inactive user accounts.				3			
	User account passwords	8.2.4	Change user passwords/passphrases.				3			
9	Back-up site security	9.5.1	Review security of the backup location.					✓		
	Media inventory	9.7.1	Conduct media inventories and properly maintain accompanying logs.					✓		
	POS POI terminal inventory	9.9.1	Maintain an up-to-date list of devices, including make, model and serial number. ★					✓		✓
	POS POI terminal security	9.9.2	Inspect device surfaces for tampering or substitution. ★						✓	
10	Log review	10.6.1	Review logs and security events of all CDE components.		✓					
	Log review	10.6.1	Review logs of other system components—as set by your annual risk assessment.						✓	
	Security control failure reporting	10.8	Implement process for detecting and reporting critical control failures. ▲ ★	✓						

> Compliance shouldn’t be seen as “fire and forget”. Maintenance is critical to security and revalidation.

REQ.	AREA	DSS 3.2	ACTIVITY	IMMEDIATELY	DAILY	WEEKLY	MONTHS	ANNUALLY	PERIODICALLY	AFTER CHANGES
11	Rogue wireless detection	11.1	Detect and identify all authorized and unauthorized wireless access points (802.11).				3			
	Rogue wireless detection	11.1.1	Maintain inventory of authorized wireless access points. ★					✓		✓
	Vulnerability scanning	11.2.1	Perform internal vulnerability scans.				3			✓
	Vulnerability scanning	11.2.2	Perform external vulnerability scans using an approved scanning vendor (ASV).				3			✓
	Penetration testing	11.3	Implement a penetration testing methodology. ★					✓		
	Penetration testing	11.3.1	Perform internal and external penetration testing.					✓		✓
	Penetration testing	11.3.4	Perform penetration tests on CDE segmentation controls (if used).					✓		✓
	Penetration testing	11.3.4.1	Confirm scope with penetration tests on segmentation controls. ▲				6			✓
	Critical file comparison	11.5	Compare critical files using change-detection mechanisms. ★			✓				
12	Security policy	12.1.1	Review security policies.					✓		
	Security policy	12.1.1	Update security policies.							✓
	Risk assessment	12.2	Perform formal risk assessment.					✓		✓
	Security awareness	12.6.1	Provide security training upon hire and at least annually.					✓		
	Security awareness	12.6.2	Confirm employees have read and understand the security policy and procedures.					✓		
	Third-party supplier mgmt.	12.8.4	Monitor the compliance status of service providers.					✓		
	Incident management	12.10.2	Review and test your incident response plan.					✓		
	Incident management	12.10.4	Train staff with security breach response responsibilities.						✓	
	Operational compliance	12.11	Confirm personnel are following security policies and procedures. ▲				3			
	Operational compliance	12.11.1	Maintain documentation of review process. ▲				3			

▲ **Service Providers only**

★ **New requirement since DSS 3.x**

Key date	**By June 30, 2018**	Replace SSL/early TLS with secure versions of each protocol. *Excluding POS POI terminals that can be verified as not susceptible to known exploits.*

Appendix D:
Security of mobile payments

While both Apple iOS and Android mobile devices use Unix operating systems, the security architecture of the platforms differs significantly. Android applications are self-signed, and available from an open app store, whereas iOS applications must be signed by Apple (for commercial use) and are available in an Apple-controlled store for applications that Apple has vetted through manual and automated means. Android applications are also installed with varying degrees of permissions, dependent upon the manifest at the time of installation.

Because Android applications are not sandboxed and have the ability to send action requests to one another, applications can use calls to determine the permission levels of other applications and use those privileges, by re-delegating permissions. Android applications are written in managed Java code, and while malicious exploits are still a concern, buffer overflows are much less of one. iOS applications, by comparison, are written in native Objective-C, which is susceptible to buffer overflows.

iOS apps, however, are sandboxed (i.e. do not have access to each other's data) and are all given the same privileges. iOS predefined APIs are the only means of communication between applications. iOS also provides built-in hardware encryption that applications can leverage, which the vast majority of Android devices do not.

Considering the foothold that Microsoft has in most enterprises, it's easy to imagine that we will see increased prevalence of active directory services hosted in its Azure cloud services, with Windows tablets and phones authenticating through Azure to fully connect them to corporate resources. Since so many POS systems are Windows-based, extending payment terminal functionality to Windows tablets and phones may be a natural evolution.

NFC, which forms the basis of most mobile wallet solutions, is a functional technology for the transmission and receipt of data. In and of itself, it isn't a complete security solution. In mobile device-as-card solutions, it is critical that payment card data that has been registered to the device is not accessible from it, either at rest or during the transmission of the data.

> “ NFC isn't a complete security system.

Technologies that secure payment card data have been improving and are a real success story for mobile commerce. Both iOS and Android have robust card emulation solutions, using an embedded Secure Element and cloud-based Host Card Emulation. Neither store card details within the device and both use tokenization to render those details worthless in isolation. Both major phone platforms are integrating their solutions with biometric authentication mechanisms that are becoming standard on most current mobile devices, further enhancing the credibility of the solutions.

Appendix E:
Methodology

Since 2008, Verizon has kept track of how many organizations manage to score 100% on their interim PCI DSS compliance validation assessment by demonstrating the ability to keep all required security controls in place all year round. The percentage of organizations achieving this milestone has steadily increased every year.

A new feature this year is data on the extent to which we analyzed compliance and the inclusion of industry vertical compliance comparisons. The following charts show the breakdown of interim Report on Compliance (iRoC) data used for this year's report by organization, industry and geography.

The data includes:

- Region Segmentation: The percentage of PCI DSS iRoCs from each geographic region.
- Vertical Industry Segmentation: The distribution of 2015 iRoC reports per industry vertical.
- Service Provider/Merchant: The percentage of iRoCs divided between service providers and merchants.

Confirmed payment card account data compromises:

- 42.6% of breaches occurred at small organizations with 11 to 100 employees.
- 20.6% of breaches occurred at medium-sized organizations with 101 to 1000 employees.
- 11.7% of breaches occurred at medium-to-large organizations with 1001 to 10,000 employees.

References to PCI DSS controls and compliance statistics in this document are based on PCI DSS 3.1 unless stated otherwise.

"Time to remediate" was calculated as the time between the date of the interim Report on Compliance (iRoC) and that of the Attestation of Compliance (AoC). It's common for organizations to remediate issues up to and during a final validation assessment and it's not until the AoC that the organization is validated to be 100% in compliance.

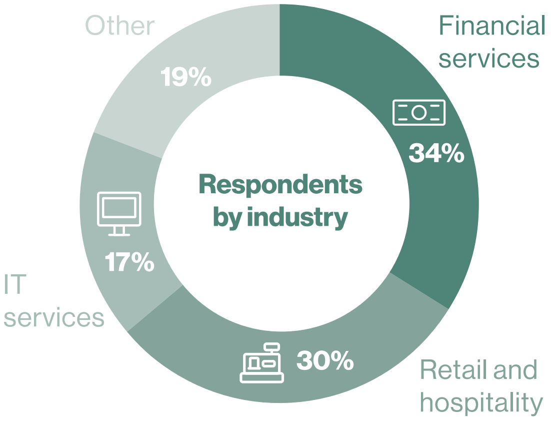


FIG 53 – Respondents by industry

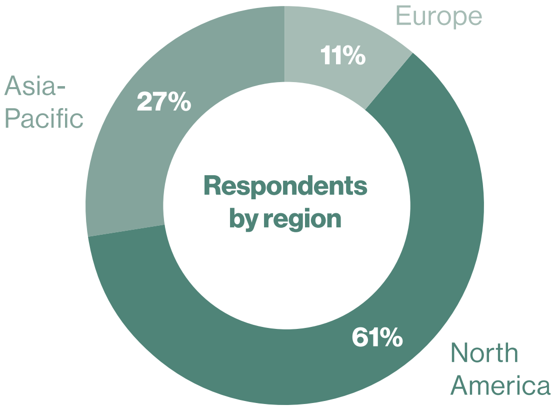


FIG 54 – Respondents by region

Verizon Security Professional Services

Verizon is a highly respected security consultancy and a trusted voice in the PCI Security community. We have one of the largest and most geographically distributed teams of QSAs, serving more than 30 countries. This gives us unrivaled insight into the state of compliance, and an exceptional understanding of what it takes to implement sustainable controls.

In the world of security, knowledge is power. The figures speak for themselves; since 2009 we've conducted more than 15,000 security assessments, many for Fortune 500 and large multinationals. Verizon has provided cardholder data security services since 2003, prior to and alongside the introduction and evolution of PCI DSS. Verizon runs one of the largest global IP networks and manages over 4,000 customer networks giving us a unique perspective on managing the operational aspects of security. On top of all this experience, we have invested in extensive research programs, publish several of the industry's preeminent ongoing research reports, and have made targeted acquisitions of leading security companies, such as Cybertrust.

> “ Verizon's security consulting organization is focused on three main areas: security assurance, cyber defense and risk management.

The PCI Security practice is part of the broader Verizon security organization, which is a leading global provider of security assurance services. We offer consulting, assessment and programs related to:

- Payment security (PCI)
- Healthcare security (HIPAA)
- Operational technologies and Control Systems (SCADA, NIST ICS)
- Vulnerability assessments (Penetration testing, Red Teaming, Code Review)
- Baseline security assessments (ISO 27000, CSC Top 20, FISMA, FedRamp)

The Verizon Cyber Defense team is a world-class provider of infrastructure security services. We help customers with assessments and improvement of existing security solutions, up to full lifecycle management of security transformation projects. With our vendor-agnostic approach, we help customers – regardless of industry – achieve positive returns on future security investment.

The Verizon RISK Team is among the world's top providers of complex incident response and digital forensics consulting services. Having performed hundreds of data breach investigations per year, the Verizon RISK Team is uniquely positioned to provide rapid response to organizations around the globe and across all industries.

> “ Verizon's PCI Security practice has been approved by the PCI SSC for QSA, PA-QSA, QSA (P2PE) and PA-QSA (P2PE) services. Verizon is also an approved PFI company.

As well as security certifications, many of Verizon's QSAs have deep industry knowledge gained from years of experience working in the retail, hospitality, financial services, healthcare and other sectors. This experience helps them appreciate your unique security and compliance challenges, and to understand your needs in the context of industry-specific security standards and regulations.

For additional resources on this research and to find out more about Verizon's PCI Security compliance services, please visit:
VerizonEnterprise.com/PaymentSecurityReport

Questions? Comments?
We'd love to hear them. Email us at:
paymentsecurityreport@verizon.com

[1] Gemalto, Customer Loyalty, Trust and Data Breaches, December 2015.

[2] Verizon, Data Breach Investigations Report, 2016.

[3] PCI SSC, Preparing for PCI DSS 3.2, February 2016.

[4] PCI SSC, Information Supplement: Best Practices for Maintaining PCI DSS Compliance, August 2014.

[5] National Institute of Standards and Technology, Directions in Security Metrics Research, April 2009. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

[6] UCLA, How to establish effective controls, 2006.

[7] CliffsNotes, Effective Organizational Control Systems, 2016.

[8] Internet retailer, Mobile commerce is now 30% of all US e-commerce, August 2015.

[9] Capgemini, IMRG Capgemini Quarterly Benchmarking: Over half of online sales now made through mobile devices, February 2016.

[10] ABI Research, Payment & Banking Card Technologies Market Data, June 2016.

[11] Visa, Secure Mobile Payment Systems, 2014.

[12] ISACA, 2015 Mobile Payment Security Study Global Results, September 2015.

[13] PYMNTS.com, Experts cast doubt on mobile payment security, September 2015.

[14] Dark Reading, Stagefright Android Bug: ‘Heartbleed for mobile’ but harder to patch, July 2015.

[15] Arxan, State of App Security Report, 2016.

[16] OWASP, Mobile Top 10 Risks 2014.

[17] TSYS, 2015 U.S. Consumer Payment Choice Study, August 2015.

[18] PYMNTS.com, MasterCard Answers The Call For Faster EMV, April 2016.

[19] PYMNTS.com, MasterCard Says Fraud Costs Dropped 54% Since (EMV) October 2015, September 2016.

[20] Smart Card Alliance, Technologies for payment fraud prevention: EMV, encryption and tokenization, October 2014.

[21] Javelin Strategy & Research, EMV in USA: Assessment of Merchant and Card Issuer Readiness, April 2014.

[22] PYMNTS.com, Walmart: EMV signatures are worthless, April 2015.

[23] PCI SSC Assessor Newsletter, November 2015.

[24] Capgemini, Top 10 Trends in Payments in 2016.

[25] Capgemini Financial Services Analysis, 2015; World Payments Report 2015.

[26] Infosecurity Magazine, The changing role of security professionals, January 2013.

Verizon 2016 Payment Security Report

Lead author
Ciske van Oosten.

Co-authors
Sky Hackett and Anne Turner.

Contributors
Charles Gatrelle, Estelle van Staden, Franklin Tallah, Ian White, Jaime Villegas, Jeffrey Cornelius, John Galt, Jyri Ryhänen, Kevin Eaton, Kevine Zerbib, Loic Breat, Marc Spitler, Paisit Thamsakorn, Pritam Bankar, Priyanka Bhattacharya, Ronald Tosto.

Editors
Cynthia B. Hanson and Rein van Koten

This report would not have been possible without contributions of data and insight from across Verizon's security practice, particularly the PCI Security and RISK teams.

Date of publication
November, 2016.

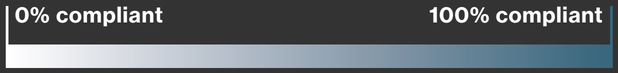
PCI Security practice management team
Eric Jolent, Franklin Tallah, Gabriel Leperlier, Ian White, Jaime Villegas, Luc Didier, Ron Tosto, Sebastien Mazas.

Intelligence manager
Ciske van Oosten.

Security practice managing director
Rodolphe Simonetti.

About the cover

The illustration on the front cover gives an overview of compliance across the 12 PCI DSS Key Requirements. Each large circle represents one of the Key Requirements, sized according to the full compliance figure – a bigger circle means more companies were compliant at interim assessment. Each of the smaller circles represents one of the base controls (like 11.2). These are shaded according to full compliance – a darker color means more organizations were compliant.



VerizonEnterprise.com