Whitepaper

Create a PCI DSS governance framework that puts you on a sustainable compliance path

Making PCI compliance part of your business

In a break from releasing updates to the PCI DSS standard every 3 years, on 28 April 2016 the PCI Security Standards Council (PCI SSC) released PCI DSS Version 3.2. Version 3.1 will expire on 31 October 2016. The PCI SSC now regards PCI DSS as a mature standard, and in general the PCI Council will stop following the defined 36-month lifecycle with new versions now being published on an as needed basis. This will align the standard with the evolving threats to the payment industry, and ensure PCI DSS controls remain fit to protect cardholder data.

Significant changes in Version 3.2 include multi-factor authentication as a requirement for any personnel with administrative access into environments handling card data, and revised sunset dates for transitioning from SSL/early TLS to 30 June 2018. PCI DSS Version 3.2 introduces a number of key changes to service providers, highlighting the importance of service provider compliance.

Stephen Orfei, PCI Security Standards Council General Manager, said “PCI DSS 3.2 advocates that organizations focus on people, process and policy, with technology playing an important role in reducing the overall cardholder data footprint.”

Troy Leach, PCI SSC Chief Technology Officer said: “Moving forward, we expect incremental revisions like those in Version 3.2 to address evolving threats to the payment landscape, with a focus on helping companies use this standard as a good framework for everyday security and business best practice.”

PCI is not an annual activity

The PCI SCC is quite right – a continuous compliance culture needs to be embedded into every organization to avoid the stressful rush to complete the annual audit. Complying with the PCI-DSS is not a goal that can simply be achieved and then forgotten about, it is an ongoing process that requires the maintenance of effective security processes, quarterly and annual security testing, and annual validation of compliance.

In fact, many organisations do not have a full understanding of PCI-DSS and believe that they are compliant when they are not, or they incur excessive costs while trying to become compliant, due to improper scope definition, the presence of cardholder data in unexpected areas, or non-completion of the validation requirements.

Organizations also tend to incur excessive costs by treating PCI-DSS compliance as a standalone project, when it can and should be integrated into an organization’s overall operational and information security processes.

Case study – the benefits of a governance framework

It pays to take a fresh look at PCI DSS, as shown in the work that NTT Security has done over three years with a Level 1 merchant who was investing multi-millions in its PCI program.

Challenge

- Despite the investment, the PCI team was frustrated that potentially significant compliance gaps still existed. Understanding that this risk was linked to the lack of a defined methodology or an agreed approach internally, they engaged the help of NTT Security to fix this.

Results

- New governance framework has resulted in a long-term sustainable reduction in compliance costs, already running into millions of pounds
- Program is seen as a pioneering change to security practices and culture within the organization
- Significant elements of the approach and principles are transferable to other areas of information security and risk, well outside the PCI DSS arena
- The investment in PCI compliance and the PCI governance framework has become a security transformation project.

The new requirements for PCI DSS 3.2 will inevitably mean more work in both understanding the requirements and then preparing for audit but, aside from this challenge of getting to grips with new standards, the annual audit itself has also become an unwelcome ritual for internal teams. It takes time, resource and budget away from other projects and is often a last minute rush, leading to mistakes, unnecessary stress and wasted energy.

The only way to break out of this cycle is to recognize that PCI DSS compliance needs to be continuously maintained throughout the year with requirements such as:

- Penetration tests – annually or following significant changes to the network
- Firewall rule-based reviews every six months
- User account reviews every 90 days
- Vulnerability scans – quarterly or after significant changes to the network
- Log reviews – carried out daily
- Application of critical security patches to all PCI components within one month of release

And although there is some latitude prior to initial compliance, there is no leeway once an organization has become compliant.

Achieving compliance for the first time can mean a significant investment and the culmination of much time and effort. And there's a tendency to think of the audit as the end point rather than just the beginning for PCI DSS compliance, with organizations relaxing once the first Report on Compliance (RoC) or Self Assessment Questionnaire (SAQ) is out of the way.

Staying compliant is as tough as achieving compliance

Becoming compliant is a huge relief but it doesn't stop there – and staying compliant can feel as tough as achieving it in the first place. Despite an organization's determination to keep on top of PCI DSS compliance requirements throughout the year, as audit time approaches it is often a struggle to find the right resources to make all the required checks before the audit deadline. In fact, organizations may even find that they cannot demonstrate the required track record of compliance and are unable to provide evidence of quarterly wireless scans or daily log reviews.

In too many cases there is a frenetic rush to validate compliance – and remedial steps are inevitably more time consuming and expensive than working towards a controlled, continuous PCI DSS compliance approach – an approach that must be understood and embedded at every necessary level of the organization.

Getting it wrong

Planning and scoping a PCI compliance program is key to its success. A poorly-planned program can have costly consequences. Programs can become extended and in some cases, organizations can spend years trying to achieve compliance. This is often due to poor advice at the outset which has resulted in incorrect scoping of the project, a mismanagement of process, and sometimes the implementation of unnecessary technology.

And of course, non-compliance can have serious financial consequences. A data breach results in a significant fine, in meeting the cost of forensic investigations and potentially large legal costs. The reputational damage as a consequence of a data breach can have incalculable financial consequences.

Practical steps to PCI DSS compliance

It's important to get your PCI compliance program right. If you don't, you can spend time, money and effort on things that you don't necessarily have to do.

For organizations working to attain PCI-DSS compliant status for the first time you'd be advised to develop a detailed pre-assessment process designed to reduce the scope of PCI DSS applicability and therefore the costs of initially achieving compliance.

Other organizations might be seeking an external, independent perspective, to ensure that they consider a wider business context and security landscape – and that PCI DSS compliance fits with other compliance requirements. Whichever path you are taking, there are some practical steps to follow.

Five things to consider when working towards PCI DSS compliance

1. Do you know where to start and how your compliance program will be sustained? The failure of most projects is due to poor advice and inability to scope the project.
2. Do you have the skills and resource in house to manage and maintain your PCI DSS compliance program?
3. Are you looking simply at PCI DSS compliance or are you thinking strategically about a wider security improvement program?
4. Do you trust the advice you have been given? Would you value a second opinion?
5. Do you know what 'good' will look like?

These practical steps include:

- Evolving a plan to ensure PCI DSS requirements are met throughout the year, and applying the knowledge of any changes to PCI standards as they happen
- Reviewing the design of any planned systems and processes to ensure PCI DSS compliance considerations are implemented before the changes are rolled out to the business
- Undertaking review and remediation support for systems, processes and business units that come into the scope of PCI DSS compliance throughout the year, rather than when the audit is looming
- Translating PCI requirements into a common, relevant language, easily understood throughout the business
- Developing interim audits, such as quarterly PCI DSS health checks, during the year to ensure that the PCI DSS program is on track
- Creating a common set of guidelines for the secure coding of payment applications
- For organizations that do not possess the resources in-house, make use of external PCI support services to address compliance gaps or perform ongoing required activities (such as vulnerability scanning, penetration testing, wireless scanning, or event monitoring).

What will good look like?

It’s important when scoping your program to understand what a good PCI DSS compliance program will look like.

A good program has sustainable compliance. It has an ongoing governance and compliance program in place, and ensures there are rigorous processes around maintaining evidence for annual audit. Technology would always be up to date, with steps in place to ensure that knowledge is transferred when people leave or move within the organization.

Managing PCI DSS compliance: In house or outsourced?

One decision you will need to make is whether to manage your compliance program in house or with the support of a third party. If you decide to engage with a third party expert, be sure to ask a few questions about their team, professional qualifications, experience and approach to the work.

- How much experience does the organization have in this area – how many PCI DSS engagements have they managed?
- Can they offer QSA pre-audit and audit support? And can they offer remediation solutions, based on a clear understanding of your business?
- What qualifications are held by the team who will support you?
- How confident do you feel with their advice?
- Do they offer a one stop shop with a full range of PCI DSS services?
- Is the organization an Approved Scanning Vendor (ASV) and Qualified Security Assessor (QSA)?

What’s important in PCI DSS 3.2?

PCI DSS Version 3.2 changes, in the main are clarifications making more obvious what the intent of a requirement is and how compliance with it is to be tested. Of the changes, the most significant include:

- Clarification that any displays of PAN greater than the first six/last four digits of the PAN requires a legitimate business need
- The introduction to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE
- Change control processes to include verification of PCI DSS requirements impacted by a change
- Revised sunset dates for transitioning from SSL/early TLS to 30 June 2018
- Inclusion of the PCI DSS Supplemental Designated Entities Validation (DESV) criteria as an appendix to the standard which was previously a separate document.

Typical PCI compliance challenges

- Lack of governance framework makes it more difficult to manage a PCI compliance program
- Staff turnover leads to gaps in knowledge transfer and processes not being followed
- Annual penetration tests started too close to the deadline to complete the remediation issues
- Firewall rules become overly complex and difficult to manage
- Issues from vulnerability scans not followed up
- Complex policies and standards with no defined timetables for regular reviews
- Network diagrams not updated after network changes.

For more information on PCI DSS 3.2 please contact NTT Security to learn more about the services available to meet all your cybersecurity needs.

About NTT Security

NTT Security seamlessly delivers cyber resilience by enabling organizations to build high-performing and effective security and risk management programs, with controls that enable the increasingly connected world and digital economy to overcome constantly changing security challenges. Through the Full Security Life Cycle, we ensure that scarce resources are used effectively by providing the right mix of integrated consulting, managed, cloud, and hybrid services – delivered by local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest information and communications technology (ICT) companies in the world. For more information, visit **www.nttsecurity.com**

To learn more about NTT Security and our unique services for information security and risk management, please speak to your account representative or visit: **www.nttsecurity.com** for regional contact information.