Payment Card Industry Data Security Standard (PCI DSS)

A roadmap to PCI compliance

A whitepaper

...making excellence a habit.™

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) covers the fundamental aspects of information security and extends through the people, processes and technologies involved in payment card processing systems.

With over 20 Qualified Security Assessors (QSAs), BSI will lead you through the PCI journey from initial review to full alignment, in the most efficient and least intrusive manner possible. Our partnership approach will allow your business to continue operating while maintaining a secure payment processing environment.

BSI's PCI DSS license is a global one and covers

- CEMEA
- EU
- USA
- APAC

This whitepaper was prepared by the BSI QSA team to help organizations better understand PCI DSS requirements and prepare for a compliance assessment. It will serve as a roadmap and provide reasonable expectations for merchants and service providers to begin or renew the process of validating compliance with the Payment Card Industry Data Security Standards.

Going through a PCI assessment can seem daunting for many organizations, especially during an initial assessment. By asking yourself the following questions and answering or being prepared to find the answer for each, the process and execution of your assessment can be simplified.

Is there commitment from executive management?

One of the most important ways to ensure that your assessment goes smoothly is to obtain commitment from top-level management that PCI compliance is a priority.

An email from the Chief Information Office (CIO) or Chief Information Security Officer (CISO) can demonstrate to the front-line personnel that will be engaged in the assessment, that their timely cooperation is vital for the success of the engagement.

Do I understand my classification and level?

It's important to understand exactly where the organization lies regarding PCI validation requirements.

Too often, companies do not know their classification or level and unknown situations present themselves during the audit, which causes delays and additional expense. First, find out whether you are a merchant, a service provider, or both.

Am I a merchant or a service provider?

From a PCI perspective, any entity that interacts with cardholder data (CHD) is either a merchant or a service provider. At a high level, a merchant is an entity that accepts CHD as payment for goods or service s and a service provider is an entity that stores, processes or transmits CHD on behalf of another entity, or provides a service that can affect the security of another entity's CHD. How is it determined whether an entity is a merchant, or a service provider? First, follow the merchant IDs.

A merchant obtains a Merchant ID (MID) from an acquiring bank, or sometimes a payment processor acting as an acquiring bank, which is used to ensure the Merchant receives the funds and that the cardholder's account is billed, for the goods or service s purchased. A more generic term for these banks or payment processors is 'acquirer', which we will use for the remainder of this paper. If an entity only stores, processes or transmits CHD using MIDs that they own, they are a merchant.

If an entity stores, processes or transmits CHD that isn't directly attached to their MIDs, they are a service provider. It's important to note that it's possible for an entity to be both a merchant and a service provider.

As mentioned above, the other way an entity can be a service provider is by affecting the security of another entity's CHD. Examples of this include hosting, managed service s and payment processing.

Why is this important? There are numerous additional PCI requirements that can require significant additional time, resources and expense for Service providers. It's critical for an entity to understand whether any of these requirements need to be assessed and to be prepared for the effort. It also lets an entity understand who needs to know they are PCI compliant.

Who needs to know I am compliant?

As previously outlined, a merchant obtains their MID from an acquirer. When an acquirer signs an agreement with the card brands allowing them to process charges, part of that contract states that they will ensure their merchants are PCI compliant. If it is determined by the brands that an acquirer's merchants are not compliant, they can be fined by the card brands.

This means, in most cases, the acquirer is the one asking a merchant to validate their PCI compliance status. In fact, in every merchant's contract with an acquirer, there is language that states they must be PCI compliant; must validate their PCI compliance. Additionally, the acquirer can pass on the fines levied by card brands to non-compliant merchants.

It's a little different for service providers. It's usually the service provider's clients asking them to show they are PCI compliant. In most cases, the service provider doesn't have a contract with either an acquirer or the card brands. However, if the service provider stores, processes or transmits CHD, they are also required to be PCI compliant. The waters are murkier for Service providers that don't handle CHD. Even if there is no contract with the brands, if a Service provider is responsible for a security breach involving CHD, they could face significant financial and legal consequences.

We've seen many cases where an entity assumed they held only Merchant status but discovered during the assessment that they were also a service provider. To avoid this, a detailed examination and understanding of the MIDs involved is required. Examine all agreements with all acquirers and compile a list of all MIDs. Finance or accounting personnel can be a helpful resource in compiling that list.

How many transactions am I handling?

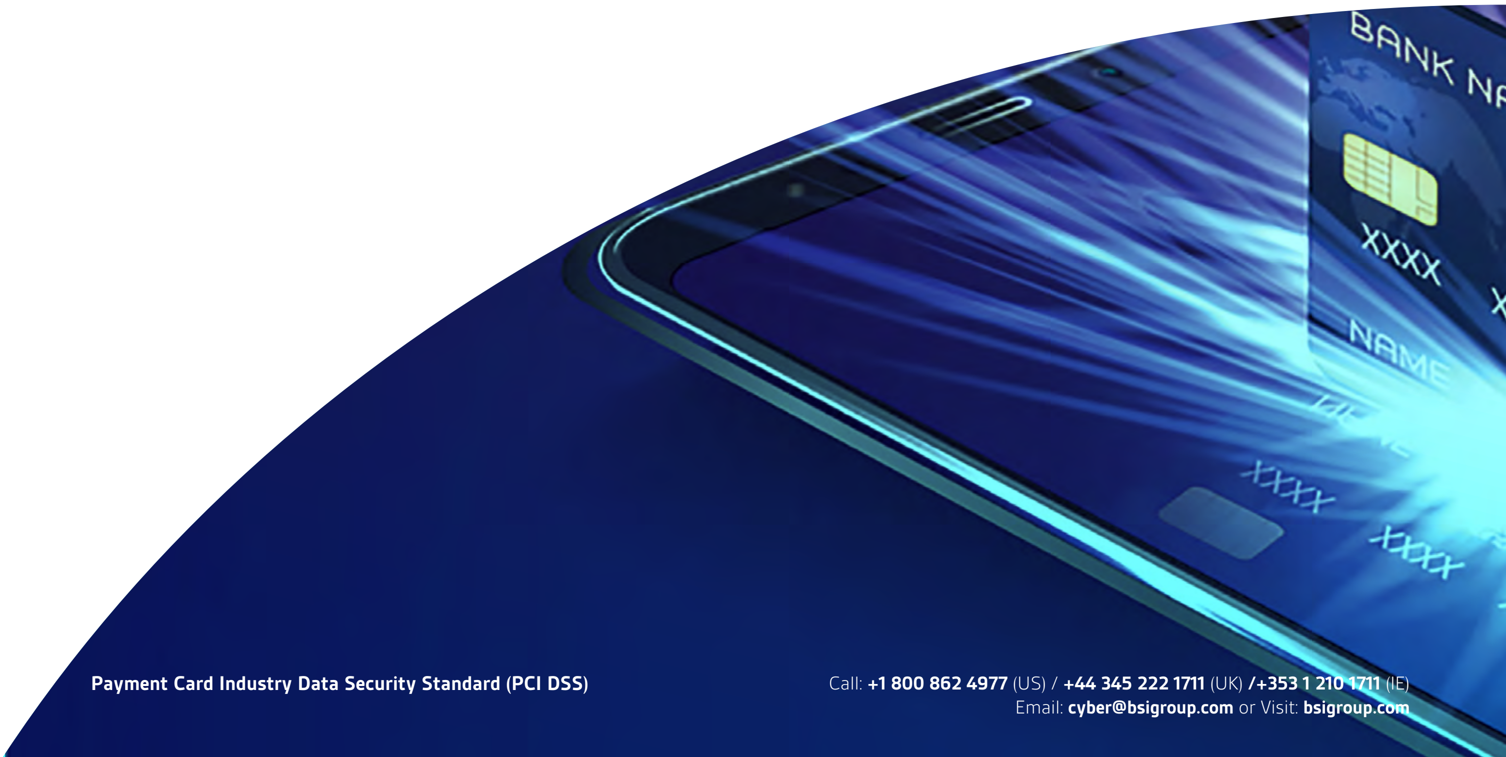
As you can see, it is critical that an entity understands which MIDs it owns, which acquirers issued them and whether they are handing CHD that is under another entity's MID. In addition to whether an entity is a merchant or service provider, the number of annual transactions handled by an entity is used to determine what they must do to validate compliance.

The card brands categorize both merchants and service providers by Levels. For both merchants and service providers, an entity with many transactions must validate compliance via an on-site Report on Compliance (ROC). Entities with a smaller number of transactions may validate PCI compliance using a variety of different Self-Assessment Questionnaires (SAQ).

Reporting templates for both of these types of assessments are available at the Council website.

Having this information in advance of any assessment helps ensure that the entity employs the appropriate validation methods. If possible, the annual transaction count should be broken down by card brand (Visa, MasterCard, Discover, American Express, JCB) as each brand has slightly different thresholds for self-assessment. Again, finance or accounting personnel can help. Additionally, this information may be obtained directly from the acquirer.

While not as common, we have seen engagements that needed change orders, because the entity was actually a different Level than they thought. The more common occurrence is that the entity is not prepared for the correct SAQ.



Do I understand my organization?

From a PCI perspective, it's all or nothing. Either an entity is compliant, or they aren't. That means it's very important to consider all portions of an entity's business. If one part of a business is compliant, but another part that is not compliant is discovered during the assessment, it can lead to added delays and costs. There are two types of entities to be considered and different approaches may be used.

Wholly owned subsidiaries

In the ROC reporting template, there is a section for listing all business entities that require compliance with PCI DSS. It specifically mentions wholly owned entities and allows the assessor to list whether each entity is included as part of the assessment or will be assessed separately. The PCI DSS glossary doesn't specifically address what wholly owned entities are, but includes this definition:

Entity	Term used to represent the corporation, organization or business which is undergoing a PCI DSS review.

Lacking any other direction, we follow the Merchant IDs (MIDs). Any entity that is using a particular MID, must be included in the same assessment. Conversely, if there is some sort of organizational unit that is somehow legally defined, it may be possible to conduct a separate assessment for that particular entity.

This is especially important for any assessment involving a Self-Assessment Questionnaire (SAQ). The SAQ templates don't include the same section specifically calling out wholly owned entities. However, there is a spot for 'Company Name' and 'Doing Business As' (DBA). This means if the company has legally defined organizational units and are using different MIDs, it may be possible to conduct separate assessments for each.

Remember, for most merchants, the acquirer is the one that sets the reporting requirements. That being the case, if there are any questions regarding which organizational units should be included in any particular assessment, consult the acquirer for direction. For service providers, consult each of the card brands.

Business units

Once the entities which require reporting have been determined, it's important to ensure that all business units of the entity are considered. It's entirely possible for a business unit to accept cardholder data without consulting IT or compliance personnel. This unexpected increase in scope can lead to delays and added cost.

Additionally, it's important to obtain input from all business units. In fact, if possible, we recommend that representatives from all business units meet to explore how each may handle cardholder data. We've found that this sort of collaboration allows the representatives to discuss ideas and suggestions, often revealing previously unknown or unconsidered cardholder data handling.

How are my organizations handling CardHolder Data (CHD)?

We established that entities handling a large amount of transactions must complete a Report On Compliance (ROC), which addresses all ways CHD is handled.

Entities without large transaction counts may opt to use one of the available SAQs. The SAQs also take into consideration how an entity handles CHD. Is it all e-commerce? Are there face-to-face transactions? Is CHD stored?

The SAQs are labeled A, A-EP, B, B-IP, C-VT, C, P2PE and D. There are separate SAQ-D documents for merchants and service providers.

This is important because each of the different SAQs has a different number of requirements. For example, SAQ-A has 22 requirements and an SAQ-D for Merchants has 330. It is important to note that SAQ-D is the only option for service providers that aren't required to complete a ROC and contains 369 requirements.

BSI has seen it happen numerous times; we discover unknown information about the environment during the assessment that ends up changing the nature of the engagement. Discovering an unknown process or system then requires more validation tasks to complete a ROC, or requires the entity to complete a much more complicated SAQ. We avoid this complication by carefully examining the scope.

What is my scope?

At a high level, the Cardholder Data Environment (CDE) which includes all people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data and all systems connected to or supporting the security of the CDE, are in-scope for the assessment. It is extremely important that each entity understands exactly how they handle CHD, or in the case of some service providers, how they are affecting the security of another entity's CHD.

Some of the items that are important to know before any engagement are:

Data flows: determine where is CHD:

- Entering
- Leaving
- Traversing systems

Payment Acceptance Channels: is CHD obtained through:

- Websites
- Mobile applications
- Telecommunications
  - Phone
  - Fax
  - Voice Over IP (VOIP)
- Postal Mail
- Email
- In person via Point of Sale/Interaction devices (POS/POI; registers, card swipes)
- Chat

CHD storage: where is CHD?:

- Stored on my systems (databases, file storage, call recordings)
- Stored by another entity (hosting providers, off-site storage)
- Backup systems (both online and backup tapes)
- Hard-copy documents

How is stored CHD protected?

- Encryption at rest and in transit
- Data destruction once no longer needed

Infrastructure: do I understand which system components are used to store, process, transmit, or protect CHD, including:

- Network devices
- Servers
- Appliances
- Other systems providing security controls (VPN servers, logging systems, etc.)
- Inventories of all system components

Service providers/Outsourcing; are outside entities:

- Storing, processing, or transmitting my CHD
- Providing other managed service s affecting the security of my CHD
- PCI compliant
- Not PCI compliant
- Providing documentation regarding which requirements are being addressed by them
- Covered by contracts which require them to protect any CHD they may posses

Personnel: do I understand those who:

- Receive CHD or enter CHD into any systems
- Can view clear-text CHD
- Have access to the CDE (cardholder data environment)
- Manage the system components
- Are roles defined and documented?

Scope reduction; to reduce scope, have I implemented

- Network Segmentation
- Payment Tokenization
- Data-loss prevention (DLP)
- PCI SSC validated Point-to-Point Encryptions solutions (P2PE)
- Other third-party solutions

Do I have a documented scoping statement?

One of the easiest ways to ensure preparedness is to assemble all the above information into a consolidated scoping statement. This describes the results of the efforts of your scope determination. It should describe the people, processes and technologies regarding how your organization handles CHD, or impacts the security of another entity's CDE

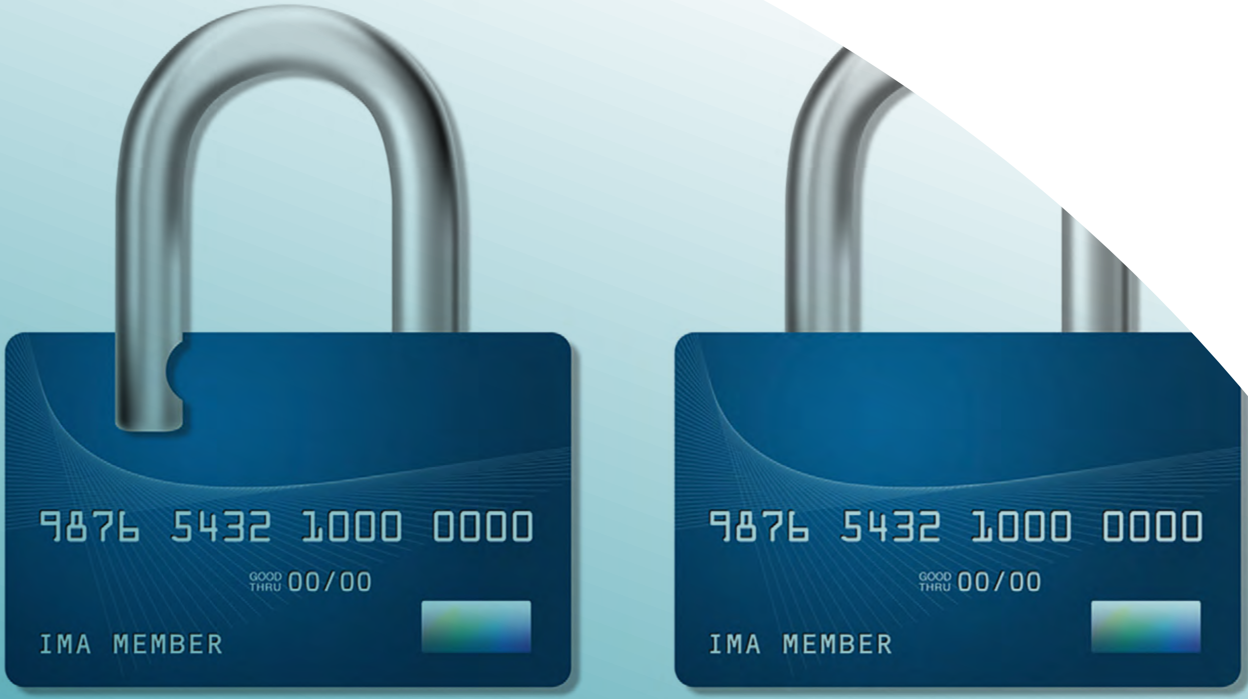
This is a valuable tool as it helps assessors understand the process by which the entity examined their environment, to ensure they know where CHD is present and where it should not be present. It can also contain evidence, or references to evidence, showing the accuracy of the scoping exercise. Finally, this sort of effort is usually done collaboratively and provides a forum where personnel can share information, which may lead to discovery of previously unknown or unconsidered possible locations of CHD.

Am I allowing enough time for my assessment?

Organizations, especially those performing a first-time assessment, frequently do not allow enough time to understand their PCI compliance responsibilities thoroughly, or to complete all of the assessment activities.

The reality is obtaining PCI compliance can be a complex undertaking. We have not even begun discussing the actual activities involved in validating compliance and previous segment have already shown that a significant time investment is required to understand the environment, organization and scope.

Availability of personnel resources is usually limited. Often, the same personnel that are handling day-to-day operations are responsible for attending interviews, obtaining or creating evidence and performing remediation activities throughout the engagement. An average Report on Compliance (ROC) takes anywhere from four to eight weeks and some self-assessments may take an equal amount of time. Careful consideration and planning before the engagement begins is critical.



Have I Considered Personnel Responsibilities?

Without good organization, things can fall through the cracks during an assessment. It's important that the following responsibilities are understood from the outset:

Scoping/overall responsibility

Service providers are required to define a PCI Charter for their PCI DSS compliance program and it must include executive management assignment of overall responsibility for maintaining PCI DSS compliance and how the PCI DSS compliance program is organized and communicated to the executive management.

For larger merchant organizations, having this sort of PCI Charter may be a good idea, or it might mean creating an oversight committee. There may also be dedicated compliance personnel who are familiar with other regulatory compliance efforts that may be enlisted.

For smaller organizations, overall PCI compliance responsibility ultimately resides with executive management.

For all organizations, as discussed previously, it's extremely important to communicate the importance of PCI compliance throughout the organization.

Interacting with business units/ requesting evidence

Ideally, compliance personnel dedicated to PCI would occupy this role. Lacking that, it should be clearly defined who will be scheduling meetings, requesting interviews and requesting evidence from relevant business units. We recommend communicating this to business units in advance and that all communication directs the business units to cooperate with the requests for interviews and evidence and provide responses to those requests in a timely manner.

Additionally, understand that whomever has this responsibility will put in as much time, if not more, than the QSA engaged for the assessment. Including this time in scheduling, workload and budgeting for the engagement is critical. BSI sees many instances where inadequate availability of this point-of-contact resource leads to delays.

Tracking

There are numerous items to track including:

- meeting and interview scheduling
- evidence requested, received, reviewed and submitted to the QSA
- outstanding items needed for the compliance of any particular requirement
- the status of remediation activities for those items found to be non-compliant

A QSA can help with tracking tools. It is also helpful to institute processes separate from the QSA, as a means of providing checks and balances. If commercial GRC (Governance, Risk and Compliance) tools are available, they may be valuable in this effort. Where they are not available, create spreadsheets that show all the applicable requirements and their status throughout the assessment.

Most often, the personnel assigned the interaction and evidence request responsibilities above are responsible for tracking the compliance status.

Interviewing

Many PCI requirements require interviews with personnel with expertize in various areas. In smaller organizations, this may be only a few people. In larger organizations, multiple personnel may be needed. The converse may also be true. For example, a single IT organization might provide authentication services to multiple business units or applications. Interviews most often address documentation and execution of different processes.

It is helpful to communicate the expected discussion topics to the business units before the interviews, so they have time to consider which personnel should be present. If there are questions regarding the interview topics, discuss it with the QSA before scheduling the interview.

Have I Considered Personnel Responsibilities?

Providing and/or creating evidence

Regardless of the environment, organization, scope, or validation documentation required for any assessment, there is evidence that needs to be supplied. In fact, just over of all of PCI requirements are documentation related.

Most often, the personnel that are interviewed are also asked to provide evidence. Depending on the type of assessment, a lot of information can be required. Types of evidence requested can include:

- Documents including network and data-flow diagrams, processes, configuration standards, industry standards, vendor manuals and patch lists, software development, change management, role definitions, physical security, inventories, vulnerability management, risk management, vendor management, training, incident response and policies
- Configuration exports from firewalls, other network devices, servers, workstations and appliances
- User lists for all facilities, system components and applications
- Logs from samples of system components
- Change records from infrastructure and applications
- Screenshots from 'shoulder-surfing' activities where the assessor is required to conduct observations
- Data captures
- Exports of production, test and development databases
- Vulnerability, risk and incident activities results
- HR activities including background checks and user termination lists

It is important that personnel are aware that they are responsible for obtaining and providing the necessary evidence. In some cases, they may be required to create evidence. For example, creating a policy or procedure that does not currently exist.

Communicate the time allowed for assembling the requested evidence. Document and track the status of each request and report the status to those responsible for overall compliance. Promptly escalate the status of delayed evidence request submission to ensure that these requests receive appropriate priority and to avoid any additional costs.

Most often, the personnel that must obtain or create this evidence are also responsible for parts of the day-to-day operations of the organization. Sufficient time and planning should be given to ensure that no delays are encountered.

Reviewing evidence

This might seem like the 'easy' part; however situations often arise where the evidence supplied is insufficient and is rejected. A good QSA will provide recommendations for correcting the evidence, but it is an unnecessary cycle of evidence re-submission.

In fact, even though it is another step in the process, reviewing evidence internally prior to submission to the QSA is actually more efficient and speeds up the validation process. Ideally, this would be done by personnel that are very familiar with PCI compliance. If no such dedicated personnel exist, a peer review can be conducted. The most important question to consider is whether the supplied evidence provides enough information to satisfy the requirement involved.

If there are questions about what is required, consult the QSA before requesting the evidence to avoid re-work.

Performing remediation tasks

Again, it's very likely that the same personnel asked to attend interviews and provide or create evidence are the ones performing day-to-day operational tasks.

Communicate the time allowed for completion of remediation activities to the personnel performing the activities. Document and track the status of each activity and report the status to those responsible for overall compliance. Promptly escalate the status of all remediation activities that might result in significant delays to ensure that these efforts receive appropriate priority and to avoid any additional costs.

How am I organizing and handling evidence?

Organization

If there are tools in place (GRC tools, document repositories, internal Wiki sites, etc.), they should be utilized. If not, an access-controlled area of a file server will usually serve the purpose. It is recommended that a structure is created that reflects the assessment. It could be a trunk for the entire enterprise, with branches for each assessment, or a single location. For full ROCs and larger SAQs, a separate location should be dedicated for each high-level PCI requirement, 1 through 12, the Appendices, Executive Summary and Miscellaneous information.

Organizing the information in this way allows for easy retrieval, including the ability to determine what was supplied in previous years.

Collection

When evidence is requested, it should be clearly communicated how that information should be provided to the requestor. If possible, there should be a single resource responsible for receiving the evidence and placing it in the proper organizational container, based on the requirement it is supposed to be addressing.

Labeling

All evidence should be labeled so it can be easily related to a general or specific requirement. An easy way to do this is to add a prefix to each piece of submitted evidence. For example:

- ES3.4_Production Network Segments
  - Note: ES is for the Executive Summary in the Report on Compliance template in this example
- 1.1.7.b_Firewall Rule Review Results
- 2.x_Windows Server Configuration Standard
- 2.x_Linux Server Configuration Standard
- 10.4_System Time Processes
- 10.4.1.a_Screenshot showing time server external sources
- A2.2_POS-POI Risk Mitigation and Migration Plan

If possible, when requesting the evidence, supply the necessary prefix for the evidence to the personnel asked to obtain the evidence.

There are occasions where the supplied evidence applies to multiple requirements. In our experience, the above labeling scheme still works, but the prefix may change year-to-year, depending on the meeting order. Retaining evidence lists and examining previous assessment efforts provide a valuable cross-reference.

Submission

When providing documentation to a QSA, it is important to ensure that confidential information is protected. QSA companies are required to ensure that evidence for PCI assessments is stored in an encrypted manner and must usually have methodologies by which documents can be securely uploaded to a repository.

If possible, a single resource should be assigned responsibility for providing evidence to the QSA.

Are there changes to the environment which must be considered?

Prior to the assessment

If this is not your first assessment, these items should be revealed during your investigation of the environment and how the organization handles CHD. It may be a good idea to document these changes in the current scoping statement, so a historical record is maintained.

Regardless of where, all changes to the environment should be documented and communicated to all relevant personnel involved in PCI compliance activities and to those with overall responsibility for PCI compliance.

During the assessment

Any changes to environment during the assessment should be avoided. It not possible, sufficient time, planning and communication is critical to avoid unnecessary re-work and delays. If possible, define and document a timeline with clear milestones as to what is going to change and when those changes will occur. Of course, clear communication with your QSA in the design phase is critical to avoid re-work and delays.

Why is this important? For example, if there are servers that are going to be decommissioned during the time of the assessment, it could be a waste of time to perform tasks such as selecting samples, requesting configuration exports, or reviewing network diagrams until after the changes are completed.

Significant change

The PCI DSS has several areas that refer to 'significant change' and provides some examples. Because organizations differ widely, sometimes even within the same entity, it is impossible to define what is 'significant' for every organization. For an entity with thousands of virtual servers, there may be automated processes that constantly spin servers up or down, depending on need, so adding a server in this manner may not be 'significant'. However, it could be very 'significant' for a small organization with only a single server to add another server.

Whether something is 'significant' or not impacts vulnerability scanning, penetration testing, risk assessments and 'significant PCI changes'. What is 'significant' for one of these areas may not be 'significant' for the others. Actions that are required for 'significant' changes are also different and potentially costly and time-consuming.

It is our recommendation that a 'Significant Change Policy' or other equivalent document is created to define what is 'significant' for each organization. Without such definition, it is up to the QSA to determine what is 'significant' or not. Delays and additional costs could result if there is a difference of opinion between the organization and the QSA.

What happens if there is an operational issue?

It's a basic tenet of compliance work: operational issues trump compliance validation efforts. Frequently, situations arise where personnel that are scheduled for an interview or have been requested to supply evidence or perform remediation tasks, are needed to address an operational issue. Usually, these sorts of occurrences are of short duration and don't result in undue delays.

Strategies to attempt to mitigate these sorts of delays may include defining backup personnel, or even back filling these personnel in advance, to free them up for compliance activities. This is more difficult in smaller organizations.

Document and report any operational issues that may cause significant delays to those with overall responsibility for PCI compliance as soon as possible, to ensure that all possible efforts are employed to avoid additional costs.

Disclaimer
BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.

Conclusion

PCI DSS often represents a significant challenge for organizations. Many companies feel overwhelmed when faced with the challenge of PCI DSS compliance and managing security in general. This feeling is only heightened due to:

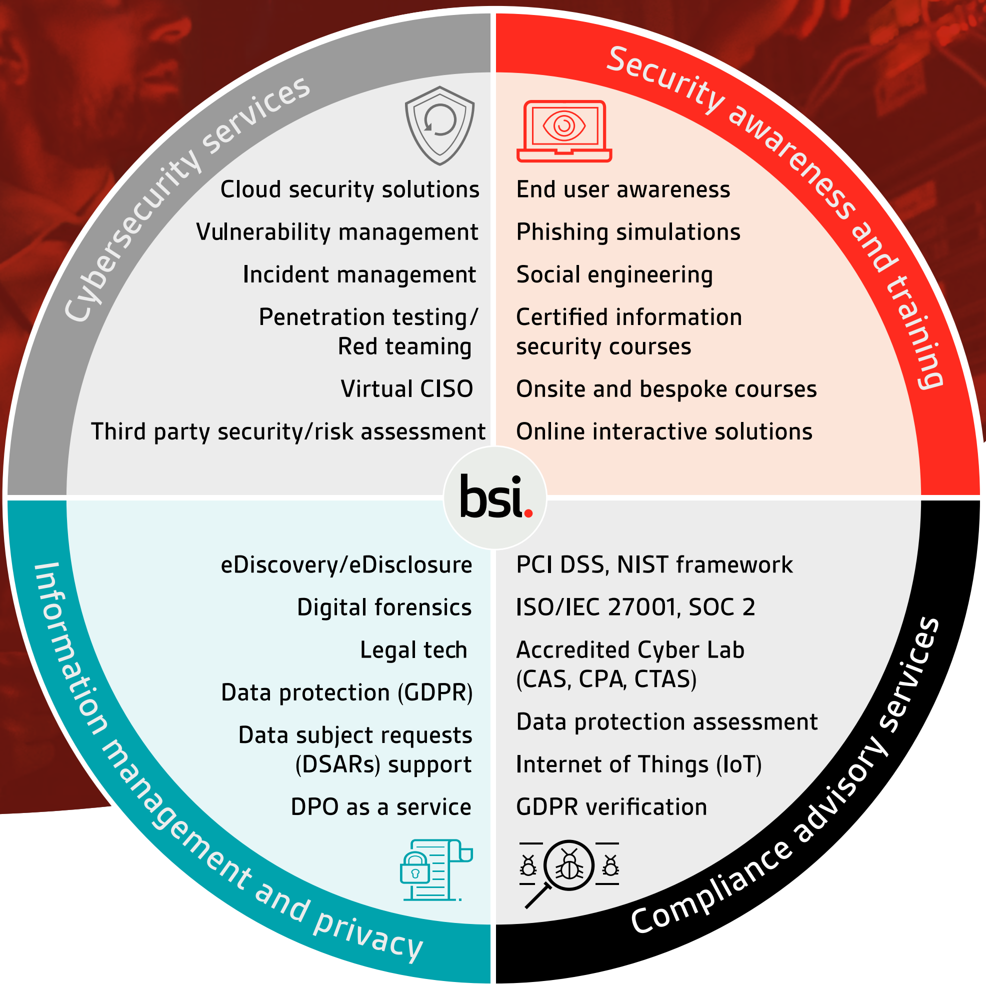
- The publicity surrounding successful cyber- attacks across the retail and ecommerce sectors
- Subsequent fines issued by regulatory agencies in Europe and the US

In the continually evolving cyber landscape, it has never been more important to ensure that your organization adopts a defensible and robust approach to cybersecurity. If you process credit card data, the de-facto standard is PCI DSS.

BSI Cybersecurity and Information Resilience

Protecting your information, people and reputation

BSI helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:



Cybersecurity services
- Cloud security solutions
- Vulnerability management
- Incident management
- Penetration testing/ Red teaming
- Virtual CISO
- Third party security/risk assessment

Security awareness and training
- End user awareness
- Phishing simulations
- Social engineering
- Certified information security courses
- Onsite and bespoke courses
- Online interactive solutions

Information management and privacy
- eDiscovery/eDisclosure
- Digital forensics
- Legal tech
- Data protection (GDPR)
- Data subject requests (DSARs) support
- DPO as a service

Compliance advisory services
- PCI DSS, NIST framework
- ISO/IEC 27001, SOC 2
- Accredited Cyber Lab (CAS, CPA, CTAS)
- Data protection assessment
- Internet of Things (IoT)
- GDPR verification

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

UK
Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com/cyber-uk

IE/International
+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com/cyber-ie

US
Call: +1 800 862 4977
Email: cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-us

bsi.