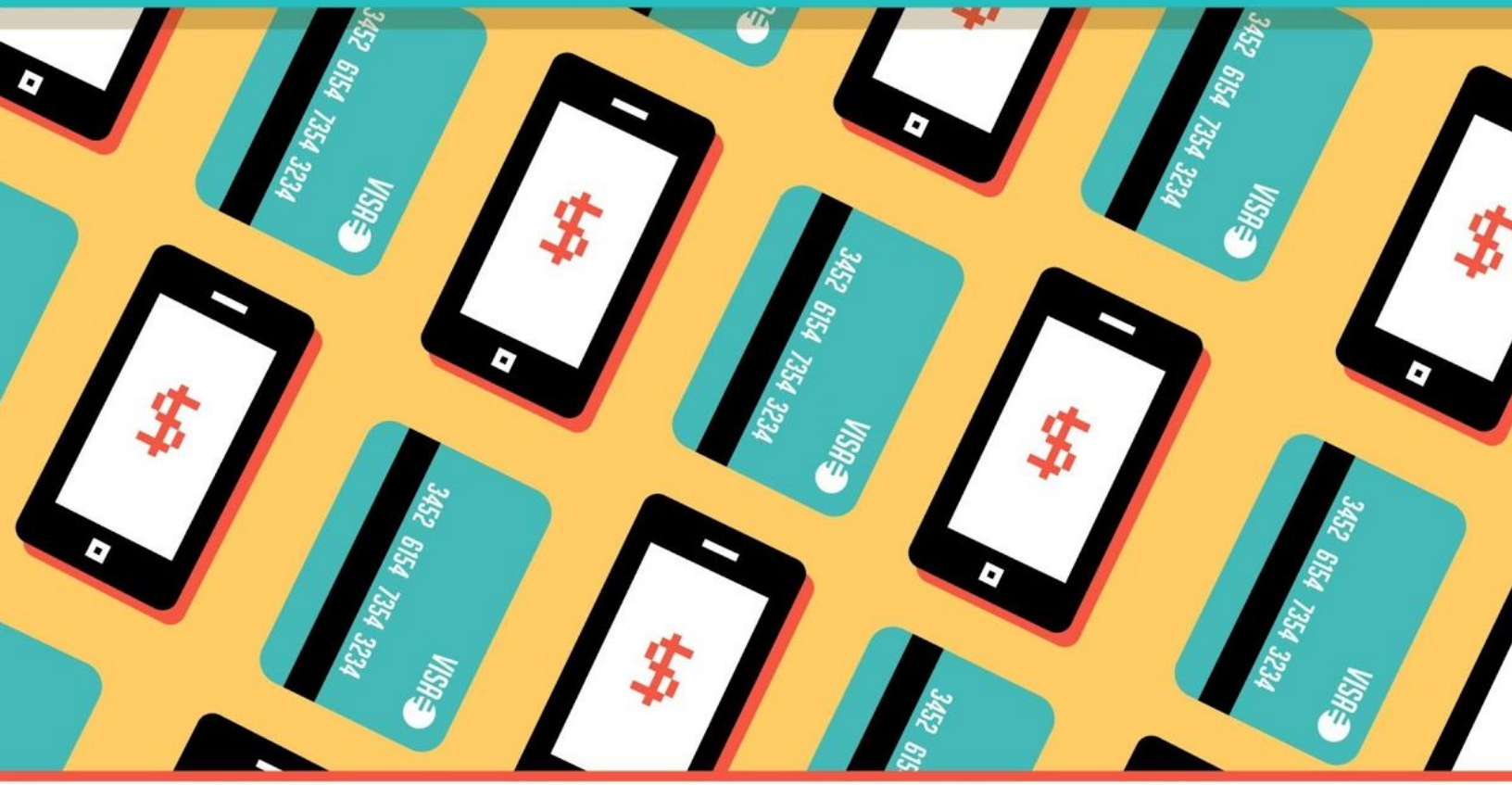
WHAT IS PCI COMPLIANCE



sas
Specialty Answering Service

sas
Specialty Answering Service

WWW.SPECIALTYANSWERINGSERVICE.NET

Contents

1 Introduction to PCI Compliance

Today the number of people who use credit or debit cards for payments has grown significantly and more than 85% of adults in the UK and more than 80% of adults in the US hold at least a debit card. In the UK alone, there are 142.8 million payment cards in issue, whereas in the US there are 576.4 million credit cards and 507 million debit cards in circulation. As a result, cardholder data security is one of the major areas of concern for the payment card industry as well as consumers today.

Willie Sutton, the notorious US bank robber, is claimed to have said that he robbed banks because "that's where the money is.'' In today's digital age, organizations handling credit card information have become vulnerable for this same reason. This is a much more serious problem as the sheer volume of data available makes the exposure much higher than the physical robbery of a bank. More than 500 million records containing sensitive information have been breached in the last decade alone and as call centers increasingly handle customers' credit card information, it is important that standard security procedures are put in place to protect cardholder data. One of the ways in which this can be addressed is to be compliant with the Payment Card Industry (PCI) Data Security Standard (DSS).

As call centers handle increasingly complex transactions and telecommunications and data networks become more complex, protecting cardholder information becomes an important strategic objective for any call center. PSCI security standards are technical and operational requirements that are set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The PCI SSC is a consortium of the five major credit card companies - MasterCard, VISA, AMEX, DiscoverCard & JCB International.

The PCI Security Standards created in 2006 includes three major standards:

1. **PCI Data Security Standard (DSS)** that apply to all entities that store, process or transmit cardholder data. It applies to merchants who accepts or processes credit cards as well as to call centers and similar third party organizations which handle customer card data.

2. **PIN Transaction Security (PTS) Requirements** which are a set of security requirements focused on devices used for payment processing related activities. It primarily applies to manufacturers of such devices. From a call center perspective, you should use only devices and components that are tested and approved by the PCI SSC for your operations.

3. **Payment Application Data Security Standard (PA-DSS)** is a set of requirements for software developers and integrators of payment applications. Your call center should ideally use PCI SSC approved software applications for credit card data processing.

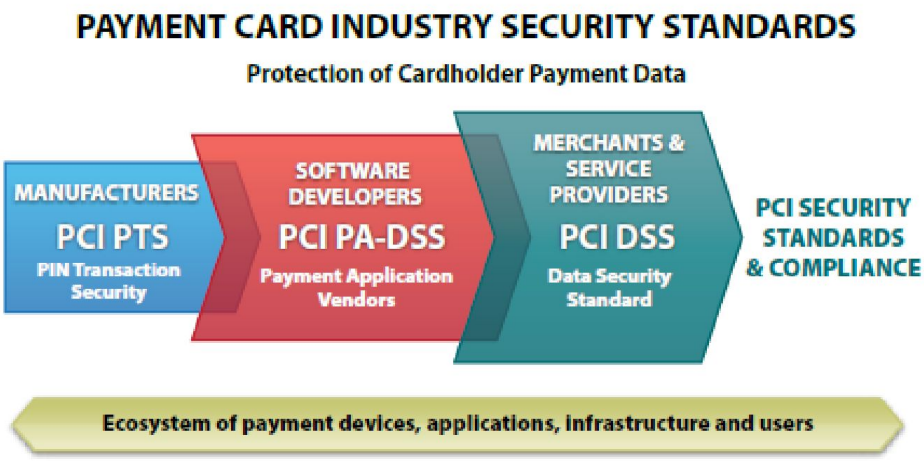


Figure 1: Ecosystem of Payment Devices (Source: PCI Quick Reference Guide)

However, when the PCI-DSS standard was initially introduced, most industry players viewed it as a necessary evil at best, as the cost of compliance was very high and penalties of non-compliance were stiff. However, high profile data breaches in recent years have made the industry realize the importance of putting tighter security measures in place.

Today, this major compliance initiative has become the de facto security standard for call centers that process customer credit card data. It has also become mandatory for anyone who accepts, captures, stores, transmits or processes credit or debit card data. The standard includes the actions to be taken to minimize the exposure for potential financial fraud. Once the appropriate measures are put in place, these need to be validated by an external certified assessor in order to attain PCI-DSS compliance.

One must remember that compliance with the PCI-DSS standard has multiple benefits – it improves consumer confidence and trust, saves penalties and fines levied by issuing banks, and also prevents revenue loss due to customer loss as well as litigation related payments. Companies who do not comply with the standard can face a fine up to $25,000 per month. In 2006, Visa imposed a whopping $4.6 million worth of fines on various parties for non-compliance with the standard. TJX Companies had to pay millions of dollars as settlement charges for a class action suit against its subsidiary TJ.Maxx and Marshalls witnessed one of the largest data breaches in recent times where nearly 94 million credit card records were compromised over a period of three years. Other companies which have experienced large data breaches in recent years include SAIC, GAP, Dai Nippon Printing and the Department of Veteran Affairs.

2 PCI Compliance Requirements

PCI DSS has six main goals or control objectives and twelve requirements, which are mapped against these objectives listed below:

Control Objectives	Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security for all personnel

Adherence to PCI DSS is an ongoing three-step process:

1. *Assess:* In this step, you identify the nature of cardholder data that you handle, the touch points in your IT systems and business processes where this data is used or stored, and then analyze these to identify potential vulnerabilities.

2. *Remediate:* In this step, you will re-engineer your process and IT assets such that vulnerabilities are fixed and such that unnecessary cardholder data is not stored anywhere in your system.

3. *Report:* In this third step, you would comply with all the requirements and submit the records necessary to validate the compliance and remedial steps taken to the acquiring bank and card brands whose data you handle as part of your operations.

In the next section, we will look at each of the control objectives of the PCI-DSS standard in a little bit more detail:

2.1 Requirements of PCI-DSS

2.1.1 Build and Maintain a Secure Network

This requirement is extremely important for a call center that handles and stores customer payment data in its network. One of the key steps to building and maintaining security is to have a firewall and router with a strong configuration to prevent thieves from hacking into your internal network. You must also have internal processes in place to perform penetration testing every time the firewall configuration is changed. All access points to cardholder data including wireless access mechanisms must be protected, and the configuration rules must be reviewed at least twice a year. The firewall and router configuration must restrict all traffic from 'untrusted' networks and hosts. It must also prohibit direct access between the Internet and any network component that handles cardholder data.

If there is a virtual working environment in your call center, it is important that even employee mobile phones, laptops and any machine that accesses your network and the data in it, have proper firewalls installed in them.

2.1.2 Do not use vendor-supplied defaults for system passwords and security parameters

This is a requirement based on common sense, as any hacker trying to gain access to your internal network is likely to try default passwords and default settings. Thus, it is vital that default passwords are changed for all your network devices including wireless devices. Configuration standards need to be developed such that they address all security vulnerabilities in your network. You must also appoint a person responsible for updating these configurations every time a new vulnerability is identified. All administrative access must be firmly restricted and passwords need to be encrypted. If you are running a hosted call center, then the hosted environment also falls under the purview of compliance.

2.1.3 Protect stored cardholder data

Cardholder data includes all the information that is printed, processed, transmitted, or stored on a payment card. Call centers that process cardholder data need to ensure that the data is protected to

prevent unauthorized use. The first rule to remember is that if your business does not need it, then do not store it. The data on the magnetic strip or chip that is used for authentication of the payment card must never be stored in your servers. If you have to store the PAN, then it has to be in an encrypted form. The encryption keys must be protected securely in order to prevent disclosure and misuse. Key management processes must be fully documented and adhered to.

When displaying the PAN in an agent's monitor, make sure to mask it and only display the first six and last four digits at maximum unless there is a genuine business need to display the entire PAN. You must also take care to purge unnecessary data on a regular basis, so that you do not store any data beyond the retention time as required by your business or legal and regulatory needs. The period of data retention must be clearly documented in your data retention policy

2.1.4 Encrypt transmission of cardholder data across open, public networks

This is especially important if you have home based agents and you are transmitting cardholder data across public networks such as the internet, GSM or GPRS. Cyber criminals have ways to intercept such transmissions; therefore, it is important that all such transcription is encrypted using strong cryptography and security protocols such as SSL/TLS or IPSec. Processes and policies should be documented such that unprotected PANs are not sent through end user messaging technologies. The call center must also have a vulnerability management program to identify weaknesses in the system that could be exploited to gain unauthorized access to cardholder data.

2.1.5 Use and regularly update anti-virus software or programs

Often malicious programs and viruses enter the internal network through email and online activities. So, it is imperative that you employ the latest anti-virus software installed on all systems including servers, home computers and mobile devices that may be used to access and process sensitive cardholder data. You must also ensure that the virus definitions are current and actively running, and that audit logs are generated periodically.

2.1.6 Develop and maintain secure systems and applications

Vulnerabilities in the IT systems and applications may expose cardholder data to unauthorized access. A lot of these can be eliminated by having a well-planned patch management program in place, guaranteeing that the latest software patches are applied on all the software. If in-house developed applications are used in your call center, then information security should be an integral part of the software development lifecycle and that secure coding practices and effective change control procedures are put in place. There must be a process established to assign a risk rank based on industry best practices to all newly identified security vulnerabilities. This will become a new requirement for PCI-DSS standards from 2012 onwards.

2.1.7 Restrict access to cardholder data by business need to know

Another key thing to maintain secure systems and applications is to have strong physical and logical access controls that restrict access to data, devices, and applications on a strict need to know

basis. Access to system components and cardholder data must be set to 'deny all' and be granted to only those individuals who require such access based on job responsibilities. The call center also needs to have a well-formalized access control policy.

2.1.8 Assign a unique ID to each person with computer access

If a data breach occurs, it is important to be able to trace the transactions to a single user. Assigning a unique ID to each person with computer access ensures that there is a proper audit trail of all actions performed. The authentication mechanism can be either based on something you know (e.g. password), something you have (e.g. smart card) or something you are (e.g. fingerprint). Remote access to the internal network must be controlled using a two-factor authentication. Password encryption is essential during storage and transmission and there should be a proper user identification and authentication for all the IT assets and software.

From a call center perspective where employee turnover rates are typically very high, it is also extremely important to have a proper process for revoking access rights for terminated and/or absconding employees. Audit trails of employees serving notice periods must be reviewed periodically to identify any suspicious transactions.

2.1.9 Restrict physical access to cardholder data

Just like technological access, physical access to cardholder data should also be restricted on a need to know basis. Facility entry controls must be in place to restrict access to the cardholder data environment. There must be mechanisms in place to monitor the physical access as well as to distinguish between onsite personnel and visitors. Visitors must be given a physical access token with a defined expiry period. A visitor log needs to be in place, maintaining an audit trail of visitor details and purpose of the visit. This data has to be retained for at least three months.

All physical and electronic media containing cardholder data must be stored in a physically secure, access-controlled environment. Media backups should also be stored in a secure location. Media must be classified based on the sensitivity of the data it contains, and there must be a well-defined policy to control the internal as well as external distribution of media. All such distribution can only be completed after appropriate management approvals are obtained. All media is to be destroyed as soon as it is no longer needed and in such a way that the data cannot be retrieved by unauthorized personnel from the destroyed media.

2.1.10 Track and monitor all access to network resources and cardholder data

Regular monitoring and testing of your physical and wireless networks is an integral part of preventing unauthorized access to cardholder data by exploiting the vulnerabilities in the network. Logs of user activity have to be maintained for effective vulnerability management, as well as to aide forensics in the event of a breach. All access to system components, especially admin access, must be clearly linked to individual user IDs, and profiles should not be shared. Audit trails of system components should be detailed enough to help reconstruct events such as individual user access to cardholder data, all actions carried out with admin privilege, any access to the audit trails

themselves, and invalid access attempts and actions around system objects. The details should include a user ID, time stamp, nature of the event, result (success/failure), data affected, and the system component affected. All system components must have time synchronization enabled and the audit trails must be secured so that they are not tampered with. The system component logs must be reviewed daily and the audit trail history must be maintained for at least one year.

2.1.11 Regularly test security systems and processes

Regular testing is essential to maintain the security of system components in your cardholder data environment. Tests should include internal and external network vulnerability scans as well as checks for any unauthorized wireless access points. These tests have to be performed at least quarterly as well as after any significant changes in the network. Penetration testing must be carried out at least annually, and after any significant change in the infrastructure. Network intrusion-detection systems must be put in place to monitor traffic at boundaries and critical points inside the cardholder data environment. File integrity monitoring tools must be deployed on a weekly basis to generate alerts in the event of an unauthorized modification of critical system or content files.

2.1.12 Maintain a policy that addresses information security for all personnel

It is important to have a strong security policy for your call center as it sets the tone for security for the entire company and makes employees aware of their duties with respect to security. It is important to sensitize your employees about the importance of protecting cardholder data. The security policy must be published and disseminated to all employees. It should also be reviewed at least once a year or when there are any significant changes. In order to minimize the risk of an internal breach of data, employees have to be background screened before hiring. Well-documented incident response plans also need to be in place to respond effectively in the event of a security breach.

3 PCI-DSS Compliance Process

The PCI Council maintains the standards on an ongoing basis. However, the compliance enforcement program varies from one payment card brand to another. While each payment card brand has its own specific requirements for validation and reporting, the broad process for compliance remains the same across the board.

The process of PCI-DSS compliance includes the following key steps:

1. *Scoping the Environment* – This step involves determining the components in the call center that should be PCI compliant.

2. *Assessment* – This involves verifying the compliance of the components in scope, either internally or by an external assessor. The assessor may also validate compensating controls in the system.

3. *Reporting* – After the assessment, the assessor or the call center submits the necessary documentation to the card issuing company or the parent company

4. *Clarifications* – If the payment card company requests for clarifications after reviewing the report, then the assessor or the call center provides the necessary clarifications and/or updates the report.

3.1 Scoping the Environment

The first and perhaps the most important step of your compliance effort is to scope the data environment for compliance. The cardholder data environment consists of technology, processes, and people who handle cardholder or authentication data. It also includes network devices, servers, software applications, and virtualization components such as virtual switches and routers as well as virtual applications and desktops. Ideally, the scoping exercise must be repeated every year before the annual assessment. You must first identify all the locations and the flow of cardholder data within the environment in order to ensure complete coverage. The areas that come under PCI-DSS can be broadly classified into three groups – organizational, technological and third party.

Organizational

The call center organizational aspects such as training of employees and background checks would need to form part of the PCI-DSS scope, as employees are a part of the scope. Policies and procedures around aspects of access control, change management, risk management and other information security areas will also form part of the scope.

Technological

This is one of the most wrongly managed areas for PCI-DSS. One needs to evaluate carefully how the network is structured in order to correctly determine the scope. The call center workstations, along

with the network of which they are a part, become part of the scope. The VOIP systems would also be part of the scope if they are used to handle calls related to cardholder data. If there is a call-recording device that records calls for training or regulatory purposes, then that also forms part of the PCI-DSS scope. Other elements in scope include the CRM database as well as everything that can communicate with it including the network infrastructure that supports it.

Third Parties

Any third parties that handle, process, or store (backup sites) cardholder data will also form a part of the scope of PCI-DSS. These third parties also need to be compliant for your call center to be compliant. If the third parties are unwilling to attain compliance, you may have to consider changing the service provider.

It is much easier to create a compliance project plan and identify the changes that need to be made in the cardholder data environment once the scope has been accurately identified. Typically, a gap analysis is performed to identify the changes needed, and this gap analysis process can be made faster and more accurate if the scoping was managed appropriately.

You can take the following steps to ensure the accuracy and appropriateness of the scope:

1. Read and understand clearly the requirements for PCI-DSS compliance by reading the standard that is available free as a download from the PCI website.

2. Understand and document all the different methods that the call center uses to access, process, and store cardholder data. Each method can be documented as a diagram with the organizational, technological, and physical elements clearly identified.

3. Before beginning the compliance process, make sure that the scope is comprehensive and nothing is missed out. Relook at the entire card lifecycle as applicable to your call center and make sure that all areas that directly or indirectly deals with cardholder data is made part of the scope.

4. Get expert advice if needed. You can engage a Qualified Security Assessor (QSA) at the scoping stage itself in order to ensure that the compliance status is not negatively impacted because of a misunderstood scope.

5. Identify and document all the cardholder data locations in your environment. After the scoping is complete, verify whether any data exists outside the currently defined cardholder data environment. The results may be documented in a pictorial form or as a list of locations.

6. Once all locations are identified and documented, make sure that all the data points are part of the assessment, unless there is any deletion, migration, or consolidation exercise that is undertaken.

7. Retain the documentation and results of how the scope was confirmed so that it can be reviewed by the assessor as well as act as a useful reference point for the next year.

3.1.1 Network Segmentation

Network segmentation allows you to isolate the cardholder data environment from the rest of the network, thus reducing the scope and making compliance easier. Reduction of scope not only reduces the cost of assessment, it also lowers the cost of compliance, as the cost and efforts for implementing and maintaining controls are lower. The best outcome of a reduced scope is that it reduces the overall risk of a data breach.

3.2 Assessment

Once the compliance requirements are met, then it needs to be validated by an audit performed by a QSA. The amount of detail and the number of criteria assessed depend on the type of merchant. The categorization of merchants and service providers vary from one credit card company to another, but in general it is based on the transaction volume. Currently VISA and MasterCard have classified companies into four levels with Level 1 applicable for companies with 6M or more transactions per annum, Level 2 for companies with 1-6M transactions per annum, Level 3 for 20,000 – 1M annual transaction volume and Level 4 for companies having transaction volumes up to 20,000. Since the risk of a data breach is proportional to the volume of data, a high volume call center will have to meet more stringent criteria. For example, while a Level 1 company needs to have an annual onsite audit done by a QSA, and quarterly network scans done by an Approved Scanning Vendor (ASV), a Level 2 or a Level 3 company needs to do only a self-assessment and quarterly network scans.

For a Level 1 company, the whole compliance exercise can cost upwards of $1 million. This huge cost is one of the reasons why companies are still hesitant to be compliant. However, companies have to realize that the cost of non-compliance can be up to twenty times more than the cost of proactive compliance.

The PCI-DSS assessor may choose a representative sample of the business facilities and system components in scope in order to assess compliance with the requirements. Though sampling is not required as per PCI-DSS, it may be used during the assessment process. However, the entire card data environment has to be compliant with all the requirements and the compliance scope cannot be reduced because of the nature of assessment sample chosen.

Compensating Controls

If there are legitimate technical or business constraints which prevent your call center from directly meeting a requirement of the PCI-DSS standard, then compensating controls may be considered, if a qualified assessor reviews and ascertains that it mitigates the risk associated with the requirement. The effectiveness of a compensating control depends on factors such as the specific cardholder data

environment in which it is implemented, the other security controls that are put in place, and the way in which the control is configured.

3.3 Reporting

Call centers need to confirm the PCI compliance with their respective payment card brands or financial institutions through official reports. Reports may include an annual attestation of compliance for on-site assessments as well as quarterly network scanning reports. Typically, a PCI-DSS annual compliance report will include the following sections:

1. *Background Information*: This will include the nature of the business conducted as well as the high level network diagram

2. *Scope and Approach:* This should cover areas such as how the scoping was done, how the assessment was made, details of network segmentation if any, sample sets selected and tested, the version of PCI-DSS for which compliance is done and so on.

3. *Cardholder Data Environment:* This section should include detailed diagrams for each network, the data flow within the system, the hardware and software in the call center, any third party applications or service providers used, the review details such as interviews conducted and documentation reviewed and so on.

4. *Quarterly Scan Results:* Details of the ASV scan results of the last four quarters.

5. *Findings and Observations:* This section should include details of findings on each requirement of PCI-DSS including validation of compensating controls.

In addition to the above, the report should also include the contact details of the call center management as well as the date of the report.

4 PCI and Call Center Operations

Today, due to the huge costs involved, data breach is a potential risk that companies are not willing to take. The only way in which a company can guarantee that there are no data breaches around payment card data is to make sure that all parties in a transaction are compliant. As a result, most organizations today expect their vendors including call centers to be 100% PCI compliant before they even shortlist them for further negotiations.

PCI-DSS compliance is a tedious task and requires a detail oriented approach for its success. The entire organization has to be committed towards compliance for ongoing PCI compliance. Compliance is easier for a single site operation as most of the network infrastructure and data would be on the premises, unlike a multi-site virtual call center, which uses home based agents. A dispersed workforce adds its own challenges. For example, protecting data as it moves from the agent's machine to the call center hub involves securing several home-office locations in addition to the central office. However, it is not impossible for virtual call centers to achieve the validation if they are process oriented and have a dedicated and knowledgeable IT team.

For call centers, especially those in the financial services domain that regularly handle cardholder data, it is important to be PCI compliant. It helps to win clients' confidence that their customers' data is protected in the call center environment. However, despite the clear advantages of PCI compliance, most call centers have chosen not to be compliant or at best, meet the very bare minimum to get the compliance certification. Today, companies that outsource their call center operations would look for the level of certification as an indication of the level of protection that their data will get. It is also important to remember that since compliance is an ongoing process, call centers must not only show that they are PCI compliant, but also have clearly laid out processes in place to ensure that compliance requirements would be met on a regular basis as well as in the future.

4.1 Planning for PCI Compliance

The relevance of PCI-DSS standards will increase in the future as organizations increasingly rely on technologies such as voice recognition and IVR to process card based transactions. Following these five steps would help your call center achieve and maintain PCI compliance on a day-to-day basis.

1. *Identify a Champion*: You have to identify a single person who would be the PCI champion in your call center. He will be responsible for seeing to it that all compliance requirements are met, and to enable your organization to adapt to the PCI way of working.

2. *Learn and Apply*: Even though the compliance requirements are the same, different call centers would approach it in different ways depending on the business objectives as well as budgetary constraints. It is therefore essential to learn about the various alternatives before you plan your compliance initiative.

3 *Train the Stakeholders*: It is important that the PCI compliance initiative is not restricted to the IT team of your call center alone. Training should be given to all operational departments – marketing, finance, the agents, and anyone else who handles customer data directly or indirectly. It is important that the C-level executives are also educated about the various aspects of compliance.

4 *Document Adequately*: You must have the security strategy and the PCI compliance program clearly documented. You must also identify the metrics to measure success and constantly monitor them.

5 *Budget Appropriately*: Every year you must earmark adequate time, money, and effort for ongoing compliance management.

4.2 Competitive Advantage of Being PCI Compliant

There are several reasons why adhering to PCI-DSS standards makes sound financial sense and here is a list of some of them.

1. *Consumers are aware of security concerns and demand a secure relationship*: While credit card companies may insist on PCI-DSS in order to control their losses, the motivation of call centers should be loss of credibility and customers in the event of a data breach. Callers expect a safe and secure transaction environment whether through a call center or an e-commerce site. Studies show that security certification improves customer confidence. Thus, you can use PCI_DSS compliance as a tool to build customer trust and loyalty. Though storing of customer transaction details may be inevitable for a call center, it is also the responsibility of the call center to protect it.

2. *Technology is constantly evolving:* PCI-DSS requirements will keep evolving as technologies such as network architecture, forensic tools, and data encryption improves. Call centers must therefore continually invest in technology, people and processes to stay compliant at all times. Remember that a small investment in a technology upgrade today may help avoid huge non-compliance related fines later.

3. *PCI standards may soon become law:* Increasingly, state and federal legislators are concerned about the security of consumer payment card data. Minnesota already has a law that holds merchants legally accountable for data security based on PCI-DSS. Other states such as California and Texas are also in the process of creating legislation around consumer data security.

In short, call centers that are proactive in their business outlook would be better off making data security a priority as it becomes critical to growth, offers a competitive advantage, and ensures financial stability.

5 Implementation Challenges

Most organizations find it a challenge to estimate the time, finances, and the effort required to implement the standard. Call centers need to relook at their PCI-DSS strategy and aim to make compliance a part of the organization's security strategy that links closely to its business strategy. This would ensure that the Board of Directors views it as a competitive advantage to be compliant and thus provide the commitment and resources needed to comply with the requirements of the standard.

One of the major hurdles to become compliant with the standard is an inability to understand the requirements of the standard. Often, organizations have to get external help from consultants or QSAs to correctly interpret the complex compliance requirements.

One of the key issues that impact effective implementation is the fact that most organizations misunderstand the scope of PCI-DSS and what it covers. QSAs who assist the organizations and act as advisors often find that there are grave mistakes in the initial phases of the project itself. As a result, the internal team of your call center may feel demotivated and frustrated. Sometimes, an incorrect scope can cause organizations to completely scrap the work done until date towards compliance and restart the efforts all over again leading to a huge waste of time and effort. Therefore, one of the key aspects of project success is to ensure that the scope of PCI-DSS requirements are clearly understood by all stakeholders from the beginning of the project itself.

Recent research has shown that call centers routinely ignore the requirements of PCI-DSS in their day-to-day operations. For example, in a recent research conducted by Veritape, a software vendor for call recording software, it was found that more than 19 in 20 call centers do not delete credit card details in their call recordings. This is a direct violation of the PCI-DSS requirement, which requires that call centers do not include card numbers and security codes in the call recordings. The survey was conducted in September 2010 and involved 133 call centers from UK, and revealed that only 3% of call centers were fully compliant with PCI-DSS. This is quite a worrying trend as there are hardware and software available today that can automatically delete credit card data from the call recordings, but most call centers still do not use them. The reasons for non-compliance vary from an ignorance of the requirements to a technical or budgetary constraints.

The problem is not restricted to call centers in the UK alone, as the "2009 Data Breach Investigations Report" from Verizon indicates. A study of the organizations where a data breach occurred revealed that only 11% of these organizations were compliant with the PCI requirements for protecting cardholder data and only 5% of the companies complied with the PCI requirements for tracking and monitoring access.

Organizations must remember that compliance is an ongoing process that requires detection and monitoring.

6 Lacunae in PCI Standard and Ways in Which PCI Can be Improved

One question was topmost in the minds of stakeholders when the large data breaches of recent years occurred. “Were these companies PCI compliant?” If they were, then it raises serious concerns about the effectiveness of PCI in preventing data breaches. In this section, we will look at some of the lacunae in the PCI standard and ways in which industry feels it can be improved.

6.1 Results are Not Public

One of the biggest concerns about the PCI-DSS standard is that there is no single body to certify the compliance efforts, as the PCI-SSC does not certify or enforce the standard. The other problem is that the credit card companies that have knowledge about which firms are compliant and which are not, do not make that information available in the public domain. At a time when consumers are worried about the security measures in place to protect their payment card information, it would be a good idea to make the compliance status publicly available. The problem with this is that the PCI-SSC does not have the resources to act as an enforcement body for the standard. There is no other eligible candidate to enforce this, either. The best solution for this will be for the call centers to voluntarily disclose their compliance status. It would help in not only increasing caller and client confidence, but will also provide a public evidence of the responsibility and commitment that the call center has towards information security.

6.2 Too Less or Too Much?

Another criticism that has been leveled against PCI-DSS is that it is too prescriptive in some areas while too vague about others. For example, the requirement for an application firewall was recently added to the PCI-DSS requirements, but the standard did not define it. As a result, most vendors of packet firewalls just added an additional layer on top of the firewall and started marketing it as an application firewall.

On the other hand, some stakeholders feel that the requirements are too tightly defined to be useful in a dynamic environment.

6.3 Independence Issues

The other problem with the standard is that QSAs who audit the organization are being paid by the organization itself. This can lead to independence issues and some companies may put pressure on the assessor to give a favorable result. There are assessors who offer consultancy services around PCI, and this adds to the ethical dilemma as the auditors themselves are selling the tools for fixing the gaps.

6.4 A Progress Indicator and Not a Benchmark

Yet another issue with PCI-DSS is that since information security is an ongoing process, PCI-DSS can only function as a progress indicator and not a benchmark. For example, most call centers have a transient employee base and as a result, the risk of a data breach is never completely eliminated.

6.5 Compensating Controls Not Good Enough

Some industry analysts also feel that the provision for compensating controls make it too lax, helping organizations to get away without doing certain things and taking measures which may not be adequate enough to provide the same level of information security. This is especially true for areas such as encryption where the standard says that encryption can be replaced with alternate controls such as internal network segmentation, two-factor authentication or IP address filtering.

If these concerns are not addressed by the PCI Council, then it is likely that the government will intervene to form federal legislation around cardholder data security.

6.6 An Ideal PCI

Given these concerns over the standard, we will look at some ways in which the standard can be improved.

The first improvement that can be brought in is to have a seal of approval so that the public has a chance to assess the service providers easily. In addition, the assessment process must be controlled directly by the Council and not just licensed by it, to bring more uniformity to the process. There should be a clear demarcation of duties between the assessor and the consultants and ideally, QSAs who audit an organization should not be allowed to provide products or consulting services to the same organization. In addition, the standards may need to be revisited more frequently than the current interval of once in two years, given the dynamic nature of cybercrimes.

The PCI standards by itself will not keep the cardholder data in a call center secure. Therefore, the onus is on the call center to have secure systems and ongoing monitoring processes in order to ensure that the data is safe.

Everyone involved in this should accept that PCI compliance is evidence that companies are using every possible means to protect against data breaches and is in no way an assurance that the data is protected against theft or fraud. Unfortunately, in this digital age, that is as close a reassurance that callers can get when it comes to the safety of their payment card data.

7 References

1. Riley, T. 2008, "In Praise of Pci", *Multichannel Merchant,* vol. 25, no. 3, pp. 46-46.

2. Carrington, C.M. 2008, "PCI Compliance: What It Means To The Call Center Industry", *Customer Inter@ction Solutions,* vol. 26, no. 10, pp. 16-17.

3. Lucas, P. 2008, "Look Out, Here Comes PCI", *Collections & Credit Risk,* vol. 13, no. 3, pp. 18-22,27

4. Genoist, H. 2006, "PCI Compliance? Priceless", *Tradeshow Week*, vol. 36, no. 12, pp. 10-10.

5. eWeek 24 Mar. 2008. "Shedding Light on PCI Compliance." *Academic OneFile*. Web. 12 Mar. 2012.

6. Conry-Murray, A. 2008, "PCI And The Circle Of Blame", *InformationWeek*, , no. 1174, pp. 31-32,34-36.

7. Georges Ataya, November 2010, PCI DSS audit and compliance, *Information Security Technical Report*, Volume 15, Issue 4, Pages 138-144.