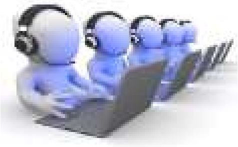
PCI DSS COMPLIANCE



A PCI DSS Compliance Checklist for Call and Contact Centers

Enterprise call and contact centers often collect, process and store a wide variety of personally identifiable information **(PII)** including payment card data, addresses, birth dates, bank account details, social security numbers, medical information and detailed address information. As a result, most contact centers fall under the scope of compliance for the Payment Card Industry's Data Security Standard **(PCI DSS).** PCI DSS was setup as an industry standard designed to help protect consumers' payment card information. It is a set of requirements that **organizations must follow in order to accept, process and transmit cardholder data {CHD}** as securely and safely as possible, in an effort to prevent fraud and reduce data breaches.

The PCI DSS is one of the most complex industry-wide standards and is constantly evolving to address the latest threats. As such, it can be costly and complicated for call and contact centers to stay on top of the newest updates and best practices for compliance. This training extract provides an initial overview, it should not be considered a comprehensive program for PCI DSS compliance.

Who Needs to Be PCI DSS Compliant

Any merchant that accepts payments must be compliant with the PCI DSS. This includes companies that accept payments and perform card-not-present (CNP) transactions over the phone, through digital channels such as online forms and web chats, or even through the mail.

Failure to comply with PCI DSS can be very costly to an organization. If a data breach occurs and the merchant is found noncompliant, the payment card brands can impose financial penalties on the merchant's acquiring bank. The bank then typically passes those costs along to the merchant, which can range from $5,000 to $800,000 per month. The payment card brands can also revoke the rights of the merchant to process transactions using their cards.

PCI DSS Requirements at a Glance v3.2 Feb 2018

Goal:	*PCI DSS Requirement:*
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.

visit the web site for more information www.kccvoip.net training@kccvoip.com

or call **EU/UK** **+44 120 766 8118** **US** **+1 646 570 1658** **Skype** **kccvoip**

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 – and ensure that all personnel are aware of it.

In More Detail

The call center and/or enterprise network will have to be logically segmented into ‘in-scope’ and ‘out-of-scope’ areas for PCI DSS. The **cardholder data environment {CDE**} is defined and drawn to show the network path of the sensitive data so that it is not necessary to audit and evaluate ALL on the company networks and devices, just the areas that carry, hold or process the sensitive data.

A vital document for PCI DSS compliance is the company **PCI Security Policy Document** - this documents all of the security procedures, CDE and logs the required tests to maintain compliance.

Requirement 1: Install and maintain a firewalls, WiFi, switches and routers configuration to protect cardholder data.

Firewalls should control the traffic allowed into and out of the various logical layers of an organization’s network, and protect the most sensitive CDE areas within its internal network. Some firewall functionality may also be incorporated within other system components such as routers and servers. Routers and switches used to connect networks are also in scope for assessment of Requirement 1 if they are used within the cardholder data environment **{CDE}.**

Organizations should establish security policies, firewall and router configuration standards that identify all connections to the CDE and log and review these configurations at least every six months. The configurations should restrict all traffic from untrusted networks and prohibit public access between the Internet and any system component in the CDE.

It is considered ‘good practice’ to utilize several firewall layers and make use of different manufacturer, type or OS at different layers so that any vulnerabilities found in one layer will not allow an intruder through all layers.

{discuss firewall and DMZ configuration}

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Should be ‘common sense’ for any security minded company….. changing the default passwords and security settings when deploying new network devices and servers, but too often people fail to take even this basic step. The default passwords and security parameters that come with new network devices are widely known, and failure to set a strong, unique password makes it easy for hackers to access the internal network. Call centers should not only change the default passwords before installing a system on the network, they should also set configurations to make sure passwords are changed and logged every time a new vulnerability is identified. This should include default passwords and security settings for wireless devices, switches, routers, firewalls and servers that are connected to the cardholder data environment or are used to transmit cardholder data.

Requirement 3: Protect stored cardholder data.

Organizations should not store sensitive data and payment card data unless it is absolutely necessary. PCI DSS states that the CVV/CVA sensitive data on the magnetic stripe or chip **must *never* be stored by an organization**. This includes voice recordings of sensitive data !

Voice recordings must be electronically masked, DTMF masking, DTMF CTI application or pause/restart to ensure sensitive data is not recorded. If using an outsourced technologies and routing the payment card data to the payment processor, the contact center is no longer processing or storing the sensitive data and its IT systems are ‘out-of-scope’ for PCI DSS.

For those contact centers that must store sensitive information, Requirement 3.4 of the PCI DSS stipulates that the primary account numbers (PAN) shown on the front of a customer’s payment card must always be rendered unreadable. Contact centers should always mask the PAN if it must be displayed for CSRs or agents, allowing only the last four digits to be displayed. Lastly, limit the storage and retention of cardholder data to only the minimum amount of time necessary for business, legal or regulatory purposes. Purge unnecessary stored data at least quarterly.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Cardholder data transmitted over open, public networks can be intercepted, so it is critical to always use encryption technologies to render the data unreadable by any unauthorized person. Call centers should use strong cryptography and security protocols such as SSL/TLS {version 1.1 or higher}, SSH or IPSec {AES or higher}, SRTP for voice traffic to safeguard cardholder data during transmission over the Internet or via wireless technologies.

Requirement 5: Use and regularly update anti-virus software or programs.

Again a ‘common-sense’ requirement in this day and age, however, many organizations are complacent when it comes to ensuring that they are up-to-date against the latest threats. Organizations must stay vigilant in ensuring that all anti-virus systems are current, actively running and generating audit logs.

Requirement 6: Develop and maintain secure systems and applications.

Hackers exploit known security vulnerabilities in systems and applications to gain access to an organization's network. Contact centers should make sure their systems have the most recently released software patches installed to help protect their systems from known vulnerabilities. They should also establish and document processes for identifying and assigning a risk ranking to all newly discovered security vulnerabilities. Perform code vulnerability reviews regularly to ensure any public-facing applications are protected against known attack methods and install firewall and Session Border Controllers SBC to protect public facing services where customers PII may be used.

Requirement 7: Restrict access to cardholder data by need-to-know.

To help prevent fraud, contact centers should ensure that sensitive PII and payment card data can only be accessed by authorized personnel and on a need-to-know basis. T his is also often referred to as the least-privilege user access (LUA) principle, which states that employees should have the minimum level of access necessary to allow them to do their job. The details should be shown in the company PCI Security Policy Document which is used to maintain compliance and for auditor reference.

Requirement 8: Assign a unique ID to each person with network and/or system access.

Another 'common-sense' security best practice that PCI DSS requires is to assign a unique identifier to each person in the organization with system access. Access can then be traced back to a specific authorized user with logs showing who did what where and when. Additionally, contact centers should implement two-factor authentication for remote access to the networks and system, such as for IT support, CSRs who work remotely, answering calls from home etc.

{discuss requirements}

Requirement 9: Restrict physical access to cardholder data.

More 'common-sense' - to ensure individuals can not access and/or remove devices, data, systems or hardcopies. Therefore, physical access to all devices and systems should be properly restricted In addition to restricting physical access to the information, one of the best methods for preventing unauthorized access is to, as much as possible, refrain from keeping sensitive data in the contact center in the first place – use CRM with direct DTMF PII entry, all stored data must be encrypted…

{discuss real terms and requirements}

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. Determining the cause of any compromise or data breach is very difficult without system activity logs and the audit trail allowing for thorough tracking and analysis if something should go wrong. All logs for systems related to security functions should be reviewed at least daily, and call centers should retain an audit trail history for at least one year. **PCI DSS dictates that at least three months of history must be immediately available for analysis.**

{Discuss SNMP vs SYSLOG vs OSSEC}

Requirement 11: Regularly test security systems and processes.

New vulnerabilities are constantly discovered. Contact centers must run internal and external network vulnerability scans at least quarterly and after any significant change in the network. They should also run external and internal penertration testing and use network intrusion detection and/or network intrusion prevention systems to monitor all traffic at the perimeter and at critical points inside of the CDE.

Requirement 12: Maintain a policy that addresses information security.

AGAIN the company PCI Security Policy Document is key - Call centers must establish, maintain and disseminate a security policy that addresses all PCI DSS requirements, an annual process for identifying vulnerabilities and formally assessing risks, and should include a review at least once a year when the environment changes. They should also have usage policies that cover remote access, removable electronic media, handheld devices, email and Internet access, remote access, password and user policies etc.

It is VERY IMPORTANT that call centers make sure that all staff, contractors and vendors are aware of these policies and procedures. Even the best data security compliance controls will not be effective if employees do not understand the importance of these policies and why they should follow them.

Contact centers must train their personnel on data security and privacy best practices and provide refreshers regularly. While most contact center employees and CSRs are good people, even good people can make mistakes that unwittingly cause a data breach or can be tempted to make a bad decision if they are under financial stress. As part of their policies, contact centers should also have in place an incident response plan so they are prepared to respond immediately in the event of a breach.

Compliance is MUCH More Than a Checklist !

Much more than simply checking a box and/or passing a PCI audit. After passing a scan for initial PCI DSS compliance, an organization must, in subsequent years, pass four consecutive quarterly scans as a requirement for compliance {depending upon merchant level}. Often the PCI Auditor is less knowledgeable than the IT staff and it can be very frustrating getting through to the auditor with the technical details - this is overcome using a good PCI Security Policy Document which can be used to explain the technical details and show the CDE clearly to any PCI Auditor.

{example CDE} discuss how and why the CDE is segmented

{example PCI Security Policy Document} discuss importance

FIPS compliance and separate function per server - discuss new PCI 3.2 requirement for similar 'separate server for services of different security level'

{add site specific details}

{discuss CVSS and how to standardize a system vulnerability}