

You Can Survive a PCI-DSS Assessment

**A QSA Primer on Best Practices for Overcoming
Challenges and Achieving Compliance**

The Payment Card Industry Data Security Standard or PCI-DSS ensures the protection of cardholder data by requiring that merchants and service providers that store, process, or transmit cardholder data meet specific security requirements. All merchants and service providers who come into contact with credit card information must comply with PCI standards, but steps an organization is expected to take to demonstrate compliance vary, based on the number of transactions processed annually.

On September 30, 2007, demonstrating compliance with PCI-DSS will become even more critical as VISA begins to levy fines against acquiring banks whose level 1 and level 2 merchants who have not demonstrated they are in compliance with the standard.

This whitepaper provides an overview of the PCI Data Security Standard and offers insight to help organizations better prepare for a PCI assessment.

How Companies Are Achieving PCI Compliance Today

PCI DSS is made up of twelve requirements that companies must follow to ensure the security of cardholder data. These requirements span every aspect of an organization's operation—from business processes to the configuration of the IT infrastructure—and many companies have implemented successful strategies to ensure compliance.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

- **What companies are doing:** To meet Requirement 1, companies are adding and/or updating firewalls, as well as performing periodic reviews and audits of firewall and router rules. For comprehensive security, firewalls must be managed effectively and documentation of firewalls configurations must be maintained and updated regularly.

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

- **What companies are doing:** Companies are disabling default passwords, hardening systems and disabling unnecessary services, and replacing non-secure protocols such as telnet with SSH and SSL.

Protect Cardholder Data

Requirement 3: Protect stored data

- **What companies are doing:** To protect stored data, companies have implemented PKI and/or other encryption solutions. They have also developed holistic data classification policies and procedures to ensure that only those who require access to confidential data—including cardholder data—can gain access. In addition, they have established data retention policies and procedures and storage methods to ensure that credit card data is retained for only as long as it is needed to meet business requirements. It is also important to review and update all policies and procedures on a regular basis.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

- **What companies are doing:** To protect cardholder data and other sensitive data that is traversing untrusted public networks, companies are implementing SSL/IPSec and wireless encryption.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

- **What companies are doing:** To meet Requirement 5, companies are deploying and updating anti-virus and anti-spyware technology, as well as ensuring that anti-virus audit procedures and logging are up to date.

Requirement 6: Develop and maintain secure systems and applications

- **What companies are doing:** Requirement 6 builds on Requirement 2 ("Do not use vendor-supplied defaults for system passwords and other security parameters") to ensure that companies keep systems and applications up to date and secure. The most successful organizations build security into their applications from the start and then update standard configurations when changes occur.

On September 30, 2007, demonstrating compliance with PCI-DSS will become even more critical as VISA begins to levy fines against acquiring banks whose level 1 and level 2 merchants who have not demonstrated they are in compliance with the standard.

To meet Requirement 6, companies are implementing and improving patch management, standard system and device builds, and change-control procedures, and are enhancing the software development lifecycle to include security. They are also reviewing and testing web application code, with many adapting OWASP standards.

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know

- **What companies are doing:** As with Requirement 2 (“Do not use vendor-supplied defaults for system passwords and other security parameters”), organizations that take a holistic approach to data security can leverage methodologies and processes to protect all confidential data, including cardholder data. Successful companies are implementing and updating strong access controls, including a “deny all” access control default strategy. In many cases, organizations are also restricting access further by providing only partial credit card data, such as the last four digits of the credit card number.

Requirement 8: Assign a unique ID to each person with computer access

- **What companies are doing:** For many organizations, meeting Requirement 8 begins with employee education to improve security awareness. All users should understand how vital it is to protect their passwords—whether they are for personal use or for business use. In addition to employee education, companies are eliminating group/batch logon IDs as part of complying with Requirement 8. They are also implementing two-factor authentication using tokens, smart cards, and biometrics, and strong user account security.

Requirement 9: Restrict physical access to cardholder data

- **What companies are doing:** To ensure physical security, companies are adding or upgrading facility access controls, using off-site media storage, and updating storage policies/procedures. For many organizations, ensuring physical security cost-effectively can be a challenge. For example, it can be expensive to deploy adequate video surveillance to record who has accessed corporate data centers. Many companies are using creative, low-cost solutions, such as installing a digital camera with a motion sensor to take pictures each time someone enters or leaves the data center.

Regularly Monitor and Test Networks

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

- **What companies are doing:** To meet Requirement 10, companies must know who accessed what data when, and from where. Centralized log servers may capture this information, but it can be challenging to review this amount of data manually, particularly if reviewing data from log servers is a daily business requirement. Implementing tools to automate the process and parse data can be very beneficial. In addition, successful companies are implementing log management, file integrity monitoring and alerting, and IDS/IPS monitoring and alerting. Importantly, companies are also maintaining and updating their log review and retention policies and procedures regularly.

Requirement 11: Regularly test security systems and processes

- **What companies are doing:** Requirement 11 closes the loop on Requirements 2 (“Do not use vendor-supplied defaults for system passwords and other security parameters”) and 6 (“Develop and maintain secure systems and applications”) by mandating testing of those systems to ensure that what has been implemented is secure. Companies test security systems and processes through vulnerability assessment scanning, penetration testing, IDS/IPS testing and monitoring, and file integrity monitoring. It is also important to complete periodic wireless assessments; even environments without authorized wireless access should ensure that there are no rogue wireless devices on the network. This may be completed efficiently with a wireless IDS/IPS. In addition, because the purpose of a PCI assessment is to scan a “representative sample” of internal systems, it can be beneficial to deploy standard system builds. Deploying a “standard” system means that fewer internal systems need to be scanned to attain an accurate sample.

Because the purpose of a PCI assessment is to scan a “representative sample” of internal systems, it can be beneficial to deploy standard system builds.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

- **What companies are doing:** To meet Requirement 12, companies are updating information security policies and incident response procedures, implementing security awareness training, and reviewing contracts with third parties who process or store cardholder data.

Securing Infrastructure Components to Ensure a Successful PCI Assessment

The most common challenges to ensuring PCI compliance center on protecting and managing data, controlling change, and auditing and enforcing policies. This section outlines best practices to ensure that infrastructure components are secure prior to a PCI assessment.

Firewalls and Routers

Best practices for firewalls and routers requires **securing firewalls at each Internet connection, demilitarized network zone, and the internal network zone**. Deny all unnecessary traffic, particularly outbound traffic for any systems that process or store cardholder data. Ideally, these systems should not have direct Internet access. Ensure that firewall rule sets are as granular as possible—right down to the port or service level—and review and document all rule sets periodically. Importantly, track all changes.

A second best practice is to **use appropriate firewall protocols**: inbound HTTP, HTTPS to web servers, SMTP to mail server, and SSH/IPSec. In addition, ensure effective log management and monitoring.

Another best practice involves **router configuration**. Look to standard configurations so all routers have a consistent build. Running configurations should be compared regularly with standards and backed up for disaster recovery, and patch management should be used consistently to identify and remediate vulnerabilities.

Servers and Workstations

These best practices apply to servers and workstations that store PAN and other cardholder information.

An initial best practice is to **build secure systems**. Document build standards and ensure that they are repeatable. Change defaults and harden servers by disabling unnecessary services. Ensure that anti-virus and anti-spyware software—with automated updates—is in place on all servers.

The most common challenges to ensuring PCI compliance center on protecting and managing data, controlling change, and auditing and enforcing policies.



Service Name	Domain Server	Start Mode	Startup Act.	Status
McAfee Framework Service	000F15A1	Manual	LocalSystem	not running
Network Associates M.S.Shield	000F15A1	Automatic	LocalSystem	not running
000F15A1 wfpdr	000F15A1	Automatic	LocalSystem	not running
000F15A1 PFS-000	000F15A1	Prohibit	LocalSystem	not running
000F15A1/00000000	000F15A1	Automatic	LocalSystem	not running
000F15A1/00000000	000F15A1	Manual	LocalSystem	not running

Figure 1. Running anti-virus and anti-spyware software is a standard best practice to ensure security. Reports like this one can identify any systems that are not running appropriate security software and pose a risk to security and compliance.

A subsequent best practice for servers and workstations is to **deploy a secure and effective patch management strategy**. Subscribe to security bulletins and newsletters, communicate information about patches to “owners” and others who may be impacted, and test patches.

Another best practice is to **ensure security testing and validation**. Run regular vulnerability scans; PCI requires quarterly scans, but a true best practice is to scan more frequently. Scan all systems prior to release to production.

A final best practice for servers and workstations is to **monitor all pertinent system activity**, including securing and managing system event logs, proactively detecting intruder activities, and monitoring file integrity.

Protecting Transmission of Cardholder Data

One best practice for protecting the transmission of cardholder data requires **strong encryption protocols**: SSL, IPSEC, private WAN (e.g., Frame Relay), and SFTP.

A second best practice is the implementation of a **strong encryption strategy**, particularly for wireless networks.

Another best practice is to ensure **email encryption configuration and management**. Ensure that there is a genuine business need to send full credit card numbers via email, and whenever possible, do not email the full PAN. In addition, ensure that users are aware of any corporate policy that pertains to sending cardholder data via email, and deploy email filters to capture outbound traffic that contains PANs.

Wireless and POS Devices

Best practices for securing wireless devices begin with consistent monitoring and vigilance. Wireless devices should be treated as “untrusted” devices and should only be used to transmit cardholder data when absolutely necessary. All default configurations should be changed, strong key encryption must be required, and a wireless IDS/IPS should be deployed. Finally, wireless access points should be physically secured.

Application Development

Security should be part of the entire SDLC process and as a best practice, **controls should be commensurate with the data to be protected**. To ensure that the development environment is PCI compliant, the development/test environment and the production environment should be fully segregated.

Additionally, a further best practice is the **integration of change management, testing, and promotion into production strategies** to ensure approval by appropriate stakeholders and to ensure that all changes are tracked.

A final best practice for application development is to **mitigate application-level security vulnerabilities** by deploying secure coding best practices (such as OWASP), thorough code review, and application-level penetration testing to close the loop. In 2008, PCI-DSS Requirement 6.6 will mandate third-party code review or an application-level firewall.

Access Control and Management

A fundamental access control and management best practice is to **manage access** through a formalized process to request authorization, and periodic review of the authorized user list and access list to find changes, such as changes in role or responsibility. Two-factor authentication should also be required for those who have remote network access.

Another best practice is to ensure the **timely removal of terminating users** through an efficient communication process and a workflow similar to that followed when users are added during the hiring process.

An additional best practice is to **frequently review user access**. This is an ideal application for an automated process. Check for users who haven't logged in for more than 90 days. (If there is a business requirement to keep such accounts on the system, disable them until they're needed.) Check for abnormal or nefarious patterns.

Domain Name	User Name
ADMIN	ADMIN
ADMIN2	ADMIN2
ADMIN3	ADMIN3
ADMIN4	ADMIN4
ADMIN5	ADMIN5
ADMIN6	ADMIN6
ADMIN7	ADMIN7
ADMIN8	ADMIN8
ADMIN9	ADMIN9
ADMIN10	ADMIN10
ADMIN11	ADMIN11
ADMIN12	ADMIN12
ADMIN13	ADMIN13
ADMIN14	ADMIN14
ADMIN15	ADMIN15
ADMIN16	ADMIN16
ADMIN17	ADMIN17
ADMIN18	ADMIN18
ADMIN19	ADMIN19
ADMIN20	ADMIN20
ADMIN21	ADMIN21
ADMIN22	ADMIN22
ADMIN23	ADMIN23
ADMIN24	ADMIN24
ADMIN25	ADMIN25
ADMIN26	ADMIN26
ADMIN27	ADMIN27
ADMIN28	ADMIN28
ADMIN29	ADMIN29
ADMIN30	ADMIN30
ADMIN31	ADMIN31
ADMIN32	ADMIN32
ADMIN33	ADMIN33
ADMIN34	ADMIN34
ADMIN35	ADMIN35
ADMIN36	ADMIN36
ADMIN37	ADMIN37
ADMIN38	ADMIN38
ADMIN39	ADMIN39
ADMIN40	ADMIN40
ADMIN41	ADMIN41
ADMIN42	ADMIN42
ADMIN43	ADMIN43
ADMIN44	ADMIN44
ADMIN45	ADMIN45
ADMIN46	ADMIN46
ADMIN47	ADMIN47
ADMIN48	ADMIN48
ADMIN49	ADMIN49
ADMIN50	ADMIN50
ADMIN51	ADMIN51
ADMIN52	ADMIN52
ADMIN53	ADMIN53
ADMIN54	ADMIN54
ADMIN55	ADMIN55
ADMIN56	ADMIN56
ADMIN57	ADMIN57
ADMIN58	ADMIN58
ADMIN59	ADMIN59
ADMIN60	ADMIN60
ADMIN61	ADMIN61
ADMIN62	ADMIN62
ADMIN63	ADMIN63
ADMIN64	ADMIN64
ADMIN65	ADMIN65
ADMIN66	ADMIN66
ADMIN67	ADMIN67
ADMIN68	ADMIN68
ADMIN69	ADMIN69
ADMIN70	ADMIN70
ADMIN71	ADMIN71
ADMIN72	ADMIN72
ADMIN73	ADMIN73
ADMIN74	ADMIN74
ADMIN75	ADMIN75
ADMIN76	ADMIN76
ADMIN77	ADMIN77
ADMIN78	ADMIN78
ADMIN79	ADMIN79
ADMIN80	ADMIN80
ADMIN81	ADMIN81
ADMIN82	ADMIN82
ADMIN83	ADMIN83
ADMIN84	ADMIN84
ADMIN85	ADMIN85
ADMIN86	ADMIN86
ADMIN87	ADMIN87
ADMIN88	ADMIN88
ADMIN89	ADMIN89
ADMIN90	ADMIN90
ADMIN91	ADMIN91
ADMIN92	ADMIN92
ADMIN93	ADMIN93
ADMIN94	ADMIN94
ADMIN95	ADMIN95
ADMIN96	ADMIN96
ADMIN97	ADMIN97
ADMIN98	ADMIN98
ADMIN99	ADMIN99
ADMIN100	ADMIN100

Figure 2. Reports such as this one validate that the accounts for terminated employees, temporary workers, or guest users have been disabled.

Physical Security

Best practices for ensuring the physical security of system components include a secure data center with limited physical access and security at retail locations. Cameras should be operational and should meet PCI storage requirements. All media—including tapes, CDs, and hardcopies—should be secured, and hardcopies should not include PANS if they are not needed. An active data retention process should be in place to ensure that hardcopies are destroyed when there is no longer a business requirement to keep them, and the data retention process should be reviewed regularly. Finally, printers and faxes that print full credit card numbers should be placed in secure locations.

Monitoring and Testing

An initial best practice for monitoring and testing is to **implement a systems monitoring strategy that provides audit and accountability**, including a centralized log server that records who, what, when, and where and is reviewed regularly. Automated tools can streamline this process.

A second best practice is to **secure audit trails and log files** in a centralized log server, which is accessed only on a need-to-know basis. Implement file integrity monitoring from the operating system to the log files.

Testing Policies and Procedures

Use port scans, vulnerability scans, and penetration testing based on requirements as a best practice for testing policies and procedures. Port scans map open ports to show which services are running. Vulnerability scans map open ports and fingerprint banners and services to determine patch levels and common defaults, and should be included in a vulnerability management program. Penetration testing uses the information gathered during port and vulnerability scanning to compromise the host.

Testing should also include file integrity monitoring on all critical hosts, IDS/IPS on all critical segments and hosts, and wireless scanning.

Data Protection

A foundational best practice for data protection is to **eliminate and purge data when it is no longer needed**. Keep cardholder data only for the length of time required for the business. You don't have to protect what isn't there!

Another best practice when data must be distributed to internal customers is to **send only relevant data**.

A third best practice for data protection is to **automate the identity process**. Build it into the HR process and include periodic access reviews.

A final best practice for protecting data is to **encrypt everywhere possible**. Evaluate encryption by platform and application and re-engineer processes where needed.

Why PCI Merchants Need Automation

- To ensure a high level of security by removing the “human” element from control to mitigate risk.
- Reduce human error in collecting configuration data.
- Provide granular configuration data to meet the requirements of multiple layers of the PCI-DSS.
- Ensure greater operational efficiency.
- Ensure accurate control measures.

PCI Requirement	Percentage of Assessments Failing
Requirement 3: Protect stored data.	79%
Requirement 11: Regularly test security systems and processes.	74%
Requirement 8: Assign a unique ID to each person with computer access.	71%
Requirement 10: Track and monitor all access to network resources and cardholder data.	71%
Requirement 1: Install and maintain a firewall configuration to protect data.	66%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	62%
Requirement 12: Maintain a policy that addresses information security.	60%
Requirement 9: Restrict physical access to cardholder data.	59%
Requirement 6: Develop and maintain secure systems and applications.	56%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	45%

Initial PCI assessments conducted by VeriSign identified requirements that posed the greatest challenge for companies facing assessment. For most organizations, protecting stored data—particularly key management and encryption—proved to be the most difficult.

Leveraging Automation to Develop an Automated PCI Compliance Process

Given the gap between growing compliance requirements and flat IT budgets, organizations are looking to automate the compliance process, particularly when it comes to collecting and auditing IT controls and policies. In fact, many of the best practices cited above can be implemented more efficiently and effectively through automated processes. A recent *InformationWeek* study indicated that “organizations with the fewest compliance problems are spending 9 percent more to automate audit functions and eleven percent less on contractors and outside services” (*InformationWeek*, December 4, 2006). Companies that automate IT security functions are reducing the cost of compliance while simultaneously improving their effectiveness in meeting compliance requirements.

As organizations become more strategic in complying with PCI, IT and business processes become integrated, allowing for fully automated reporting. Importantly, when a PCI compliance strategy incorporates standardized, integrated, and automated processes, continuous PCI compliance becomes a part of the way an organization does business, rather than a one-time “event.”

In addition, organizations implementing a centralized CMDB to provide a single repository for data connection gain greater control over configuration changes in their environment. By increasing visibility into their infrastructure, not only are these organizations more likely to pass their PCI assessment, they also reap benefits in areas of security, performance and overall system availability. Finally, a CMDB allows testing and reporting to be streamlined across the entire infrastructure, eliminating the workload and expense of manual identification, and paves the way for maintaining a continuous compliance strategy.

Automation Lowers Costs

- Streamline PCI testing and reporting
- Reduce resource load and money spent on compliance
- Reallocate PCI compliance resources back to key IT initiatives
- Increase reporting accuracy, repeatability, and frequency
- Produce systemic, audit-ready configuration reports

Preparing for PCI—before an Assessment Begins

Ecora provides software and services that allow organizations to implement sustainable, automated PCI compliance programs.

One service Ecora offers is a PCI Gap Analysis. Typically a two- to three-day engagement, this service collects a sampling of configuration data from across operating systems, database management systems, directories, applications, mail servers, network devices, and firewalls, and then compares the data against appropriate control requirements found in the PCI Data Security Standard. The resulting analysis provides actionable information that can be used to remediate deficiencies.

To learn how Ecora's Gap Analysis or other Ecora software and services can help you automate detailed reporting for PCI assessments and other regulatory compliance audits and enabling IT best practices, call [877.923.2672](tel:877.923.2672) or [+1 603.436.1616](tel:+1603.436.1616), email sales@ecora.com, or visit us on the web at www.ecora.com.

About Ecora Software

Ecora Software provides Enterprise Configuration Visibility™ to customers worldwide, ensuring their IT infrastructures are secure, compliant and effective. Ecora is the market-proven leader in transforming enterprise-wide configuration data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's flagship solution, Auditor Professional™, provides the only patented architecture proven to automate the collection and reporting of configuration information from the entire infrastructure, without agents. Ecora Software takes the cost and complexity out of compliance audits and adopting IT best practices for more than 3,600 customers, including many of the Fortune 100. For more information, please visit Ecora at www.ecora.com.

