

Payment Card Industry
Data Security Standard (PCI DSS)

Compliance Planning Guide

Version 1.2

Published: July 2007

Updated: October 2009

For the latest information, please see
microsoft.com/technet/**SolutionAccelerators**

Copyright © 2009 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, BitLocker, Excel, Forefront, Hyper-V Server 2008 Server, Internet Explorer, MSDN, SharePoint Server 2007, SharePoint Services, SQL Server 2008, Visual Studio, Windows, Windows 2000, Windows Server, Windows Server 2008, Windows Server 2003, Windows Vista, and Windows XP are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Executive Summary 1](#_Toc231720500)

[Introduction 2](#_Toc231720501)

[Who Should Read This Guide? 3](#_Toc231720502)

[What Is the Payment Card Industry Data Security Standard? 4](#_Toc231720503)

[Planning for PCI DSS Compliance 5](#_Toc231720504)

[The PCI DSS Assessment Process 6](#_Toc231720505)

[Automating PCI DSS Requirements 8](#_Toc231720506)

[Document Management 8](#_Toc231720507)

[PCI DSS Automation Recommendations 8](#_Toc231720508)

[Available Technologies 8](#_Toc231720509)

[Risk Assessment 10](#_Toc231720510)

[PCI DSS Requirements Automated 10](#_Toc231720511)

[Available Technologies 10](#_Toc231720512)

[Change Management 13](#_Toc231720513)

[PCI DSS Requirements Automated 13](#_Toc231720514)

[Available Technologies 13](#_Toc231720515)

[Network Security 14](#_Toc231720516)

[PCI DSS Requirements Automated 15](#_Toc231720517)

[Available Technologies 15](#_Toc231720518)

[Host Control 18](#_Toc231720519)

[PCI DSS Requirements Automated 18](#_Toc231720520)

[Available Technologies 18](#_Toc231720521)

[Malicious Software Prevention 20](#_Toc231720522)

[PCI DSS Requirements Automated 20](#_Toc231720523)

[Available Technologies 20](#_Toc231720524)

[Application Security 21](#_Toc231720525)

[PCI DSS Requirements Automated 22](#_Toc231720526)

[Available Technologies 22](#_Toc231720527)

[Messaging and Collaboration 23](#_Toc231720528)

[PCI DSS Requirements Automated 23](#_Toc231720529)

[Available Technologies 24](#_Toc231720530)

[Data Classification and Protection 25](#_Toc231720531)

[PCI DSS Requirements Automated 25](#_Toc231720532)

[Available Technologies 26](#_Toc231720533)

[Identity Management 27](#_Toc231720534)

[PCI DSS Requirements Automated 27](#_Toc231720535)

[Available Technologies 27](#_Toc231720536)

[Authentication, Authorization, and Access Control 29](#_Toc231720537)

[PCI DSS Requirements Automated 29](#_Toc231720538)

[Available Technologies 30](#_Toc231720539)

[Vulnerability Identification 31](#_Toc231720540)

[PCI DSS Requirements Automated 31](#_Toc231720541)

[Available Technologies 31](#_Toc231720542)

[Monitoring, Auditing, and Reporting 32](#_Toc231720543)

[PCI DSS Requirements Automated 32](#_Toc231720544)

[Available Technologies 32](#_Toc231720545)

[Managing PCI DSS Technology Solutions 33](#_Toc231720546)

[Available Technologies 33](#_Toc231720547)

[Summary 34](#_Toc231720548)

[Appendix 35](#_Toc231720549)

[Frequently Asked Questions 35](#_Toc231720550)

[Additional Resources 36](#_Toc231720551)

[Feedback 37](#_Toc231720552)

[Acknowledgments 38](#_Toc231720553)

[Contributors and Reviewers 38](#_Toc231720554)

# Executive Summary

If your organization processes, stores, or transmits payment cardholder information associated with American Express, Discovery Financial Services, JCB International, MasterCard Worldwide, or Visa Inc. International, it must comply with the Payment Card Industry Data Security Standard ([PCI DSS](https://www.pcisecuritystandards.org/)). The requirements defined in this standard, which were developed by the PCI Security Standards Council, are designed to create the minimum acceptable level of security for cardholders who use your organization’s services.

Achieving compliance with PCI DSS can be challenging, and can significantly affect your organization’s business processes, service architecture, and technology solutions. For example, in order to establish a fully functional, documented and enforced PCI DSS compliance strategy, it is important to centrally coordinate compliance efforts across your organization. Guidance that can help your organization with these efforts is available in the Governance Risk and Compliance (GRC) Service Management Function, as well as other service management functions (SMFs) in [Microsoft Operations Framework (MOF) 4.0](http://go.microsoft.com/fwlink/?LinkId=42590). Organizations must also consider what GRC authority documents apply to them, and how overlaps in control objectives can be addressed as efficiently as possible. Complying with multiple sets of regulations will likely require additional research to determine whether there are overlapping requirements that mandate a separate set of controls. Such complexities can make it difficult to understand how to respond appropriately to different regulatory requirements, as well as how to do so in a cost-effective manner. Compliance to regulatory, industry standard, and client-issued requirements affect the organization’s ability to effectively conduct business, and may be measured differently.

The *Payment Card Industry Data Security Standards (PCI DSS) Compliance Planning Guide* is designed to help individuals who are responsible for addressing PCI DSS requirements in their organizations. The purpose of this guide is to help IT managers understand how they can start to address many IT control requirements that apply to their organizations, including PCI DSS compliance requirements. The guide also provides information about technology solutions that can help facilitate this process.

For a broader discussion about how to comply with multiple regulatory standards, see the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419)*.*

**Important**   This planning guide does not provide legal advice. The guide only provides factual and technical information about PCI DSS. Do not rely exclusively on this guide for advice about how to address your regulatory requirements. For specific questions, consult your legal counsel, GRC subject matter expert, and PCI assessor.

# Introduction

The *PCI DSS Compliance Planning Guide* is designed to help organizations address the requirements of version 1.2 of the Payment Card Industry Data Security Standard (PCI DSS). Specifically, this guide is intended for merchants that accept payment cards, financial institutions that process payment card transactions, and service providers—third-party companies that provide payment card processing or data storage services. IT solutions for each of these groups must address all PCI DSS 1.2 requirements.

This guide is intended to extend the[*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419), which introduces a framework–based approach to creating IT controls as part of your organization’s efforts to comply with multiple regulations and standards. The [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419) also provides configuration and operation guidance for Microsoft products and technology solutions that you can use to implement a series of IT controls to help address PCI DSS requirements, as well as many other regulatory obligations that your organization may have.

**Important**   This planning guide does not provide legal advice. The guide only provides factual and technical information about PCI DSS. Do not rely exclusively on this guide for advice about how to address your regulatory requirements. For specific questions, consult your legal counsel, GRC subject matter expert, and PCI assessor.

This guide includes the following sections:

* **Executive Summary**. This section provides a broad overview of the PCI DSS requirements and the primary goals of the guide. It discusses the knowledge that IT managers need to start addressing their PCI DSS compliance requirements.
* **Introduction**. This section offers a brief overview of the guide, PCI DSS, and the intended audience for this guide in the following subsections:
* **Who Should Read This Guide?** This section describes the audience for the guide, the guide’s purpose and scope, and caveats and disclaimers about the limitations of this guidance.
* **What Is the Payment Card Industry Data Security Standard?** This section provides an overview of PCI DSS and its requirements.
* **Planning for PCI DSS Compliance**. This section introduces how to use a framework to address PCI DSS requirements. This approach includes creating various types of IT controls, how these controls work in combination, and why they are important components that your organization can use to help address PCI DSS requirements and other regulatory compliance obligations.
* **The PCI DSS Assessment Process**. This section provides an overview of the PCI DSS assessment process that Qualified Security Assessors (QSA) use to evaluate an organization’s compliance with PCI DSS requirements.
* **Automating PCI DSS Requirements**. This section describes Microsoft technology solutions that your organization might consider as it plans to address PCI DSS requirements. A series of subsections take advantage of a MOF–based approach to help ensure that planning, deployment, and monitoring are done in the most effective manner.
* **Summary**. This section provides a brief summary of the guide.
* **Appendix**. This section provides a list of frequently asked questions, additional resources, and an invitation to provide feedback on the guidance.
* **Acknowledgments**. This section recognizes the team that developed this guide, and the efforts of contributors and reviewers.

Because this guide is a supplement to the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419)*,* Microsoft recommends to reference both guides when planning a complete solution to help address all applicable regulatory requirements for your organization.

Note   If your organization provides automatic teller machines (ATMs) as part of its service offerings, Microsoft provides architectural and security guidance for the software, systems, and networks that support ATMs. For more information, see the Microsoft [Banking Industry Center Downloads](http://msdn2.microsoft.com/en-us/architecture/86e3451d-8219-46af-bf99-4a610e4bf1f4.aspx) page on the MSDN® Web site.

## Who Should Read This Guide?

The *PCI DSS Compliance Planning Guide* is primarily for individuals who are responsible for ensuring that their organizations collect, process, transmit, and store cardholder data securely and reliably, while maintaining cardholder privacy. Typically, these responsibilities are addressed by individuals serving in one or more of the following roles:

* **Chief Information Officers (CIOs)** who are concerned with the deployment and operation of systems and IT-related processes.
* **Chief Information Security Officers** **(CISOs)** who are concerned with the overall information security program and compliance with information security policies.
* **Chief Financial Officers (CFOs)** who are concerned with the overall control environment of their organizations. This is often delegated to financial positions such as those in Payments Operations, and Accounts Receivable.
* **Chief Privacy Officers (CPOs)** who are responsible for the implementation of policies that relate to the management of personal information, including policies that support compliance with privacy and data protection laws.
* **Technical Decision Makers** who determine the appropriate technology solutions to solve certain business problems.
* **IT Operations Managers** who run the systems and processes that execute the PCI DSS compliance program.
* **IT Security Architects** who design the IT control and security systems to provide an appropriate security level to meet the business needs of their organizations.
* **IT Infrastructure Architects** who design infrastructures that can support the IT security and controls that IT Security Architects design.
* **Consultants and partners** who recommend or implement privacy and security best practices to achieve PCI DSS compliance objectives for their customers.

In addition, the following individuals might also find this guide to be helpful:

* **Risk/Compliance Officers** who are responsible for the overall risk management of meeting PCI DSS requirements for their organizations.
* **IT Audit Managers** who are concerned with auditing IT systems and reducing the workload of internal and external IT auditors.
* **Auditors** who are responsible for inspecting, validating, and attesting to the compliance of PCI DSS.

For more details about key roles and responsibilities, refer to the MOF 4.0 Team SMF, which identifies key roles and responsibilities in an IT operations environment.

## What Is the Payment Card Industry Data Security Standard?

PCI DSS is a set of comprehensive requirements designed to ensure that cardholder credit and debit card information remains secure regardless of how and where it is collected, processed, transmitted, and stored. Developed by the founding members of the PCI Security Standards Council—including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.—PCI DSS helps protect credit card customers through established business and technical best practices and encourages international adoption of consistent data security measures.

Additional information about PCI DSS is available on the [About the PCI Data Security Standard (PCI DSS)](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml) page of the PCI Security Standards Council's Web site.

PCI DSS version 1.2 is the most recent version of the standard, and supersedes all previous versions of PCI DSS. The standard is organized into the following group of six principles and 12 requirements. Each requirement contains subrequirements for which you must implement processes, policies, or technology solutions to comply with the requirement:

* Build and Maintain a Secure Network:
* Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
* Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
* Protect Cardholder Data:
* Requirement 3: Protect stored cardholder data.
* Requirement 4: Encrypt transmission of cardholder data across open, public networks.
* Maintain a Vulnerability Management Program:
* Requirement 5: Use and regularly update antivirus software.
* Requirement 6: Develop and maintain secure systems and applications.
* Implement Strong Access Control Measures:
* Requirement 7: Restrict access to cardholder data to business need-to-know.
* Requirement 8: Assign a unique ID to each person with computer access.
* Requirement 9: Restrict physical access to cardholder data.
* Regularly Monitor and Test Networks:
* Requirement 10: Track and monitor all access to network resources and cardholder data.
* Requirement 11: Regularly test security systems and processes.
* Maintain an Information Security Policy:
* Requirement 12: Maintain a policy that addresses information security.

Requirements 9 and 12 do not demand that you implement technology solutions. Requirement 9 instructs you to address the physical security of the locations where cardholder data is stored and processed. Addressing this requirement could include implementing building access security, installing and maintaining surveillance equipment, and requiring identity checks for all individuals who work at or visit your facilities. Requirement 12 instructs you to create an information security policy and disseminate it to your employees, vendors, and any other parties within your organization who work with cardholder data.

## Planning for PCI DSS Compliance

It is neither efficient nor cost-effective to create PCI DSS compliance solutions in isolation from other applicable GRC objectives. Other regulations must be considered when planning your approach to such compliance solutions, including the following:

* [Sarbanes-Oxley Act (SOX)](http://www.sarbanes-oxley.com/section.php)
* [Gramm-Leach-Bliley Act (GLBA)](http://www.ftc.gov/privacy/privacyinitiatives/glbact.html)
* [Health Insurance Portability and Accountability Act (HIPAA)](http://www.hhs.gov/ocr/hipaa/)
* [European Union Data Protection Directive (EUDPD)](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)
* [ISO 27002 Code of Practice for Information Security Management (ISO 27002)](http://www.27000.org/iso-27002.htm)
* [American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP)](http://infotech.aicpa.org/Resources/Privacy/Generally%2BAccepted%2BPrivacy%2BPrinciples/Generally%2BAccepted%2BPrivacy%2BPrinciples/)
* [North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection](http://www.nerc.com/page.php?cid=6%7C69) *(CIP)*

Note   If your organization is a multinational business, or accepts transactions from international locations, you should have a discussion with your GRC subject matter expert to ensure that it is in compliance with governmental regulations for all locations where you do business. Microsoft suggests to also consult legal counsel with knowledge of all regulations for the locations where your organization does business.

For more information about the planning, delivery, and operation of compliance efforts for each of these regulations, see the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419)*.*

PCI DSS compliance solutions should be developed with full awareness of existing solutions that satisfy other regulatory requirements. To accomplish compliance goals efficiently and effectively, Microsoft recommends that you use a control framework to map applicable regulations and standards, which will help your organization be more efficient through a harmonized set of controls. Details on effective frameworks that can help address your organization’s regulatory compliance objectives are available in the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419).

Using the [Microsoft Operations Framework](http://go.microsoft.com/fwlink/?LinkId=42590) (MOF), you can take advantage of several service management functions that help to organize compliance efforts. The Plan phase of MOF contains the Business/IT Alignment, Reliability, and Policy service management functions. Use these functions to determine how your organization may take advantage of IT to meet the compliance needs of a business in a reliable and policy-driven manner. The manage layer contains the Governance, Risk, and Compliance Service Management Function, which focuses on meeting the goals of compliance through proper resourcing and analysis of business value. After installing a compliance framework, you can map new regulations and standards affecting the organization to it. You can then efficiently concentrate your efforts on those parts of the framework in which requirements have changed.

A framework provides many significant benefits for organizations seeking to achieve their compliance objectives. A framework–based approach to compliance allows organizations to accomplish the following:

* MOF: Governance, Risk, and Compliance SMF — Combine IT controls to address multiple regulatory standards, such as those from PCI DSS and EUDPD, and reduce duplicate audit preparation activities.
* MOF: Business/IT Alignment SMF — Prioritize spending by choosing IT controls that will achieve the most impact.
* MOF: Change and Configuration SMF — Avoid duplicate work by knowing the current state of your configurations and reduce the risk of negative impact from changes to the organization.
* MOF: Change and Configuration SMF — Update current regulations more efficiently through incremental changes to your organization's existing IT controls.
* MOF: Team SMF — Establish a common ground between the IT department and auditors.

Review PCI DSS prior to planning your compliance efforts to meet the standard. The PCI Security Standards Council's Web site provides a helpful Portable Document Format (PDF) file titled [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf). In addition, the Council has created a [New Self-Assessment Questionnaire](https://www.pcisecuritystandards.org/saq/index.shtml) that can help your organization determine whether it is in compliance with PCI DSS. You can also use it to help plan your organization’s PCI DSS compliance efforts. The PCI Council has also provided guidance for [prioritizing](https://www.pcisecuritystandards.org/education/prioritized.shtml) how to achieve DSS compliance.

For more information about addressing regulatory requirements using IT controls in a control framework, see *the* [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419)*.*

For more information about supporting documentation for PCI DSS 1.2, such as a summary of changes made to version 1.1 of the standard, and general FAQs, see the [Supporting Documents PCI DSS V1.2](https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml) page.

## The PCI DSS Assessment Process

The audit process for PCI DSS compliance is generally similar to the process outlined in the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419). However, a few details that are specific to PCI DSS auditing in this section might be useful to your IT staff.

[The PCI SSC New Self-Assessment Quiestionnaire (SAQ)](https://www.pcisecuritystandards.org/saq/index.shtml) contains a tiered audit formula to determine what type of audit is required of your organization. Factors include the role of your organization (service provider or merchant), and data elements and monthly transaction volume processed by your organization. Answers to these questions determine whether a self-audit is sufficient, or whether an onsite audit and attestation is required by a qualified third-party organization. Consult the PCI DSS Applicability Information, Scope of Assessment for Compliance with PCI DSS Requirements, and Additional PCI DSS Requirements for Shared Hosting Providers sections of PCI DSS for further information. Then complete the [Self-Assessment Questionnaire](https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf) (PDF) to determine what level of audit is required of your organization. The logical diagram at the end of this questionnaire can assist you in determining your audit requirements.

PCI DSS audit reviews are performed by two types of third-party organizations, known as Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs). QSAs perform the onsite portions of an audit, while ASVs perform vulnerability scans of your organization’s Internet-facing environments. Organizations that become QSAs and ASVs must be reviewed and approved by the PCI Security Standards Council (PCI SSC) once a year.

The QSA is required to prepare a report on Compliance (ROC) after auditing your organization that must follow specific guidelines defined by the PCI DSC. These guidelines are contained in a [Security Audit Procedures](https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf) (PDF) document for merchants on the PCI Security Council's Web site. Service providers and merchants must complete an [Attestation of Compliance](https://www.pcisecuritystandards.org/saq/docs/aoc_service_providers.doc) document (Microsoft® Word document), which is also available from the Council's Web site.

The guidelines specify how to organize the report that the QSA must file after the audit. This report includes the contact information for your organization, the date of the audit, an executive summary, a description of the scope of work, as well as the approach the QSA took in auditing your organization, quarterly scan results, compensating controls (if any), and the QSA’s findings and observations. The last section contains the bulk of the information about your organization’s compliance with PCI DSS. In this section, the QSA uses a template to report on your organization’s compliance with each of the PCI DSS requirements and subrequirements.

As you plan for and schedule PCI DSS audits for your organization, your legal counsel, GRC subject matter expert, internal auditor, and the IT management of your organization should review PCI DSS audit procedures as identified. A project scope best practice can be found in MOF section 3.2 Project Plan. Using this information can help you fully understand what the QSA will review during your audit.

The ASV must also prepare a report on the results of their vulnerability scans on your organization’s Internet-facing environments. Guidelines for this report are contained in a [Security Scanning Procedures](https://www.pcisecuritystandards.org/security_standards/supporting_documents.shtml) (PDF) document available on the PCI Security Standards Council's Web site posted in the PCI DSS Security Scanning Procedures section of the supporting documents. This document specifies what elements of your organization’s environment the ASV must scan and includes a key to help you read and interpret the ASV’s report.

As a merchant or service provider, your organization must follow each payment card company’s respective compliance reporting requirements to ensure that they acknowledge your organization’s compliance status. Each payment card company has slightly different compliance rules and procedures. For more information about specific PCI DSS compliance requirements, and the support programs each company offers to enable merchant and service provider compliance, contact the payment card companies for which your organization processes, transmits, or stores cardholder data.

# Automating PCI DSS Requirements

This section describes Microsoft technology solutions that your organization might consider when it plans for PCI DSS compliance. Incorporate the solutions that you choose into the everyday workings of your organization. As mentioned in the "Planning for PCI DSS Compliance" section earlier in this guide, your organizational policies, processes, procedures, and technology solutions should address regulatory compliance across your entire organization, and you should consider how PCI DSS compliance will affect all parts of your organization.

For a detailed discussion of the considerations involved in mapping IT controls to technology solutions, see the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419) and other related guidance in the [Regulatory Compliance TechCenter](http://go.microsoft.com/fwlink/?LinkId=91315) on Microsoft TechNet. In addition, using [Microsoft Operations Framework 4.0](http://go.microsoft.com/fwlink/?LinkId=42590) can provide integrated best practices, principles, and activities that will help guide your organization through the best service-oriented functions using well-defined service management functions (SMFs) that are grouped to better address all phases of service management. Your organization can take advantage of a MOF–based approach to help ensure that planning, deployment, and monitoring are done in the most effective manner.

For example, a PCI review will often involve the use of external help. To ensure that contractor resources are well utilized and managed correctly, MOF 4.0 provides valuable guidance for engaging them in an optimal method.

## Document Management

Document management solutions combine software and processes to help you manage unstructured information in your organization. This information might exist in many digital forms, including documents, images, audio and video files, and XML files.

### PCI DSS Automation Recommendations

Implementing document management solutions helps with PCI DSS compliance in two ways. For example, using such solutions to manage documents that contain cardholder data can help address PCI DSS requirements that relate to data access, management, and protection. Specifically, you can use document management solutions to meet requirement 7 and subrequirement 10.2.1. You also can use document management systems to maintain and publish policies, such as those required to fulfill Sections 3.6, 6.4, 9.2 and 12.

For the full text of each of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers a number of technologies that you can use together or independently to create IT controls for document management. Design these controls to meet PCI DSS requirements, as well as any other regulatory requirements that are applicable to your organization.

* **Microsoft Windows® Rights Management Services**. Windows Rights Management Services (RMS) is a software platform that helps applications safeguard digital information from unauthorized use—both online and offline, and inside and outside of the firewall. RMS is the foundational technology behind the Information Rights Management (IRM) features of Microsoft Office and Windows SharePoint® Services. An RMS server, either deployed in-house or accessed through a hosted service, is required to use these features.

RMS can augment your organization's security strategy by protecting information through persistent usage policies, which remain with the information no matter where it goes. You can use RMS-enabled applications to manage, control, and audit access to documents that contain card holder information. The RMS client is integrated into the Windows Vista® operating system. For other versions of Windows, the RMS client is available as a free download.
For more information, see [Microsoft Identity and Access Solutions](http://www.microsoft.com/rms).

* **Microsoft Office SharePoint® Server**. SharePoint Server is a collaboration and content management server that allows you to use one integrated platform to support the portal and document management needs of your organization. It allows you to support intranet, extranet, and Web applications across your enterprise, and provides your IT professionals and developers with the platform and tools they need for server administration, application extensibility, and interoperability. You can use SharePoint Server as a central repository for documents that contain cardholder data, as well as for documents that describe policies and processes. SharePoint® Server 2007 is integrated with RMS, so that access control policies can be enforced on all copies of content downloaded from SharePoint Server 2007. This feature enables site administrators to protect downloads from a document library with IRM. When a user attempts to download a file from the library, Microsoft Windows SharePoint Services verifies that the user has permissions to the given file, and then issues a license to the user that enables access to the file at the appropriate permissions level. Windows SharePoint Services then downloads the file to the user's computer in an encrypted, rights-managed file format. Microsoft recommends to store credit card information in an encrypted database, not in documents in a collaboration environment. Policies, procedures, audit information, and the PCI DSS could be stored in the collaborative environment to facilitate controlled and efficient access to required information.
For more information, see the [Microsoft Office SharePoint Server 2007](http://go.microsoft.com/fwlink/?linkid=12632) Web site.
* **Microsoft Exchange Server**. For most organizations today, e-mail is the mission-critical communications tool that employees must use to produce their best results. This greater reliance on e-mail has increased the number of messages sent and received, the amount and variety of work performed by e-mail, and even the speed of business itself. Exchange Server provides a rich messaging platform to manage information exchange in your organization while helping meet PCI DSS compliance objectives. Exchange Server 2007 includes unified messaging, which consolidates e‑mail, voice mail, and faxes sent to a user into a single inbox. It also offers features that enable your organization to apply retention rules, scan and act on messages in transport, flexibly journal, and perform rich text searches across all deployed mailboxes.
For more information, see the [Microsoft Exchange Server](http://www.microsoft.com/exchange/default.mspx) Web site.
* **Microsoft Office**. Office is the premier suite of productivity applications for organizations. The Information Rights Management (IRM) feature of Microsoft Office helps organizations control access to sensitive information such as cardholder data.

Specifically, the Office IRM feature helps your organization accomplish the following:

* Prevent authorized recipients of protected information from forwarding, copying, modifying, printing, faxing, or cutting and pasting the information for unauthorized use.
* Prevent protected information from being copied with the Windows Print Screen function.
* Provide information with the same level of protection wherever it goes, which is referred to as *persistent protection*.
* Provide the same level of protection to e-mail attachments, as long as the attachments are files created with other Office programs, such as Microsoft Excel® or Microsoft Word.
* Protect information in e-mail messages or documents that have been set to expire, so that the information can no longer be viewed after a specified period of time. Enforce policies that govern the use and dissemination of information within and outside the organization.

For more information, see the [Microsoft Office](http://office.microsoft.com/en-us/help/HP062208591033.aspx) Web site.

## Risk Assessment

Risk assessment is the process by which your organization identifies and prioritizes risks to your business. Typically, you use a systematic method to identify the assets of an information-processing system, the threats to those assets, and the vulnerability of the system to those threats. In the context of regulatory compliance, risk assessment is the process of assessing the level of compliance and compliance inadequacies within your organization. When planning for PCI DSS compliance, your primary concern is to identify risks to cardholder data and prioritizing the mitigating solutions to those threats.

### PCI DSS Requirements Automated

Risk assessment can help you address PCI DSS requirements in a number of ways. It allows you to identify the areas in your network that need to be upgraded to achieve compliance. Even after you have achieved initial compliance, risk assessment is important in determining whether your organization stays in compliance over time. Because you can use risk assessment to address many potential issues, it can help you achieve compliance with many of the PCI DSS requirements, including requirements 1, 3, 4, 5, 6, 7, 8, and 11.

For full text of each of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers a number of technologies that you can use together or independently to create IT controls for risk assessment. Design the following controls to meet PCI DSS requirements, as well as other regulatory requirements that are applicable to your organization:

**Microsoft Security Assessement Tool (MSAT)**. A free tool that provides organization with the ability to assess weaknesses in a working IT environment. MSAT provides guidance, reveals a prioritized list of issues, and helps provide specific guidance to minimize those risks. MSAT is an easy, cost-effective way to start strengthening the security of your computing environment and your business. Begin the process by taking a snapshot of your current security state, and then use MSAT to continuously monitor your infrastructure’s ability to respond to security threats. MSAT consists of over 200 questions covering infrastructure, applications, operations, and people. For more information about the MSAT tool, see the [Microsoft Security Assessement Tool](http://technet.microsoft.com/en-us/security/cc185712.aspx) page on TechNet.

* **Microsoft Baseline Security Analyzer (MBSA)**. One of the primary tools you can use to assess risk to cardholder data in your organization is the MBSA tool. This easy-to-use tool identifies common security misconfigurations in a number of Microsoft products, including Microsoft Windows operating systems, Internet Information Services (IIS), SQL Server®, Microsoft Internet Explorer®, and Microsoft Office. The MBSA tool also scans for missing security updates, update rollups, and service packs published to Microsoft Update. You can run the MBSA tool from the command prompt or in its GUI, and you can use it with Microsoft Update and Microsoft Windows Server® Update Services. Because keeping your systems current is a very important way to make cardholder data as secure as possible, the MBSA tool can be invaluable for assessing data risk in your organization.

For more information about the MBSA tool, see the [Microsoft Baseline Security Analyzer](http://technet.microsoft.com/en-us/security/cc184924.aspx) page on TechNet.

* **Microsoft Systems Management Server**. If your organization uses Microsoft Systems Management Server (SMS) to manage client computers and servers, you may already have some of the tools you need to perform risk assessment for cardholder data. With SMS, your organization can remotely manage security settings on computers running Windows operating systems over distributed networks. You can inventory whether computers on your network have installed required software updates and track the progress of update rollouts to those computers. SMS also enables you to generate reports that identify your full hardware and software inventory, the configuration details and status for computers on your network, and the status of software deployments and deployment errors. These SMS features can be very important in assessing risk to cardholder data within your organization.

For more information about SMS, see the [Microsoft Systems Management Server](http://www.microsoft.com/smserver/default.mspx) home page.

* **Microsoft System Center Operations Manager Audit Collection Services (ACS)**. Operations Manager 2007 can securely and efficiently extract and collect security logs from computers running Windows operating systems and store them for later analysis and reporting. The extracted logs are stored in a separate Audit Collection server database. Operations Manager ships with reports that you can use for ACS data. You can use Audit Collection to produce various compliance reports, such as supporting Sarbanes-Oxley audits. You also can use ACS for security analysis, such as intrusion detection and unauthorized access attempts.

For more information, see the [Audit Collection Services (ACS)](http://technet.microsoft.com/en-us/library/bb381258.aspx) page on TechNet.

* **Windows Server Update Services**. Windows Server Update Services with Service Pack 1 (SP1) enables your organization to deploy many of the latest Microsoft product updates published to the Microsoft Update site. Windows Server Update Services is an update component of Windows Server and offers an effective and quick way to help keep systems up to date. WSUS provides a risk assessment infrastructure that consists of the following:
* **Microsoft Update**. The Microsoft Web site to which WSUS components connect for Microsoft product updates.
* **Windows Server Update Services server**. The server component that is installed on a computer running Microsoft Windows® 2000 Server SP4, Windows Server® 2003, or Windows Server® 2008 inside the organization's firewall. Windows Server Update Services server provides the features that administrators need to manage and distribute updates through a Web-based tool, which can be accessed from Internet Explorer on any Windows computer in the organization's network. In addition, a Windows Server Update Services server can be the update source for other Windows Server Update Services servers.
* **Automatic Updates**. The client computer component built into Microsoft Windows 2008, Windows Vista, Windows Server 2003, Windows® XP, and Windows 2000 SP3. Automatic Updates enables both server and client computers to receive updates from Microsoft Update or from a server running Windows Server Update Services.

These services enable you to provide all host environments on your network with the latest security fixes from Microsoft for the products installed on the given host.

For more information, see the [Microsoft Windows Server Update Services](http://go.microsoft.com/fwlink/?LinkId=71054) page on TechNet.

* **Group Policy**. Group Policy is a capability that enables IT professionals to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to Active Directory® Domain Services (AD DS) containers such as sites, domains, and organizational units (OUs). You can centrally manage computers across a distributed network using Group Policy. Because your administrators can use Group Policy to distribute software across a site, domain, or range of OUs, it can be an important tool for determining risks to your organization’s IT environment.

You can use the Microsoft Group Policy Management Console (GPMC) to manage Group Policy settings. The GPMC is designed to simplify the management of Group Policy by providing a single place for managing core aspects of Group Policy. GPMC addresses the top Group Policy deployment requirements, as requested by customers, by providing the following:

* A user interface (UI) that makes Group Policy much easier to use.
* The ability to backup and restore GPOs.
* The ability to import and export, and copy and paste GPOs and Windows Management Instrumentation (WMI) filters.
* A simplified way to manage Group Policy–related security.
* The ability to generate HTML reports for GPO settings and Resultant Set of Policy (RSoP) data.
* The ability to script GPO operations that are exposed by the GPMC—but not the ability to script settings within a GPO.

For more information about Group Policy, see the [Windows Server Group Policy](http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx) page on Technet, and [Introducing the Group Policy Management Console](http://www.microsoft.com/windowsserver2003/gpmc/gpmcintro.mspx). Consider using the GPOAccelerator as part of the [Security Compliance Management Toolkit Series](http://technet.microsoft.com/en-us/library/cc677002.aspx) to deploy recommended security settings for your environment. Using this tool can save you hours of work that you would otherwise need to configure these settings.

## Change Management

MOF Change and Configuration Management is a structured process by which your organization assesses changes to a project plan, an IT infrastructure, software deployments, or other processes or procedures in your organization. A change management system can help you define a change, evaluate the impact of the change, determine what actions are required to implement the change, and disseminate information about the change across your organization. It can also help you track the changes you make in your organization and help you maintain control of your IT environment as you make changes to it.

For example, a change management system could involve a database to help personnel make better decisions about future changes based on historical data that indicates the success or failure of similar changes that have been tried in the past. Change management is also a structured process that communicates the existence and status of changes to all affected parties. The process can yield an inventory system that indicates what actions were taken and when the actions affect the status of key resources, which can help predict and eliminate problems and simplify resource management.

### PCI DSS Requirements Automated

Change management is as critical to PCI DSS compliance as it is to any other regulatory compliance effort. If your organization does not know what changes it has made to its IT environment, it is difficult to claim with any certainty that the environment is secure. Tracking changes in your network, systems, policies, and procedures helps you to meet PCI DSS requirements 6 and 11.

For the full text of each of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers multiple technologies for you to consider when designing your change management solutions.

* **Microsoft Office SharePoint Server 2007**. In addition to being a technology option for your document management solutions, Microsoft Office SharePoint Server 2007 can also be a key element in a change management system for your organization. You can use its version tracking capabilities to monitor changes in policy and process documents, updates and other changes to applications, and changes in approved software over time.

For more information, see the Document Management section and the [Microsoft Office SharePoint Server 2007](http://www.microsoft.com/sharepoint/default.mspx) Web site.

* **Microsoft Systems Management Server**. Not only can you use SMS to manage risk assessment for your organization, you can also use its management features to track changes in computer systems across your organization. SMS tracks security setting changes as well as applications installed on servers and client computers across the network. You also can use the powerful reporting functionality built in to SMS to review the changes that have been made to computers in your organization and whether these changes address the security requirements you have established.

For more information about SMS, see the [Microsoft Systems Management Server](http://www.microsoft.com/smserver/default.mspx) page on TechNet.

* **Microsoft SMS 2003 Desired Configuration Monitoring 2.0**. You can augment your SMS operations with the SMS 2003 Desired Configuration Monitoring (DCM) feature. You can use DCM to automate the configuration management audits between desired or defined configuration settings and actual configuration settings. DCM accomplishes this by allowing users to define desired hardware, operating system, and application configuration settings in multiple configuration data sources. Then, using the supplied auditing engine, DCM compares desired settings with actual settings and reports configuration compliance.

DCM can help you to reduce unplanned service downtime, correlate configuration data, and reduce support costs. It provides you with an easy-to-use XML editing tool and guidance for defining hardware and software configuration items. DCM also provides detailed compliance reports to help detect and remediate configuration errors.

The [Security Compliance Management Toolkit Series](http://technet.microsoft.com/library/cc677002.aspx) provides DCM Configuration Packs that provide security baselines for Windows Server 2008, Windows Server 2003, Windows Vista, Windows XP, and Microsoft Office 2007. The purpose of the toolkit series is to reduce the work required to manage DCM configuration baselines that maintain recommended security settings for different operating systems from Microsoft. For more information about how to baseline Microsoft products in your environment, see the guidance provided in each toolkit of the series.

* **Microsoft Desktop Optimization Pack for Software Assurance**. The Microsoft Desktop Optimization Pack for Software Assurance is a subscription service that reduces application deployment costs, enables delivery of applications as services, and provides better management and control of enterprise desktop environments. The desktop optimization pack allows you to enhance change management processes and rollbacks through:
* Improved Group Policy management.
* Reduced downtime.
* On-demand access to applications for approved users.

The Microsoft Desktop Optimization Pack is available only to customers with Software Assurance coverage on their desktops. For more information, see [Optimizing the Windows Desktop](http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/optimizeddesktop.mspx).

## Network Security

Network security solutions constitute a broad solution category designed to address the security of all aspects of an organization's network, including firewalls, server computers, client computers, routers, switches, and access points. Planning for and monitoring the security of your organization’s networks is a key element of achieving PCI DSS compliance. Although there are many solutions available to address network security, your organization should already have many of the elements of a secure network in place as a matter of course. It is likely more efficient and cost-effective to build from the network security solutions you have already implemented than to begin anew.

However, you might consider changing some technologies that your organization uses, or you might want to implement new solutions that you have not already included in your network security strategy. Microsoft offers several technology solutions and guidance materials for implementing network security solutions to help address the needs of your organization.

### PCI DSS Requirements Automated

The Payment Card Industry Data Security Standard (PCI DSS) is very clear in stating that you need to establish secure networks throughout your organization to achieve compliance. Requirement 1 states that to be compliant, an organization must build and maintain a secure network. Requirement 1 states that organizations must install and maintain a firewall configuration to protect cardholder data. Requirement 2 states that organizations must change the vendor-supplied default settings for system passwords and other security parameters. Network security solutions also help your organization meet Requirements 4 and 10, which mandate that organizations encrypt transmission of cardholder data across your network and that you track and monitor network access, respectively.

For the full text of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers a number of technologies to address the first two PCI DSS requirements.

* **Windows Firewall**. Windows Firewall is a built-in, host-based, stateful firewall that is included in Windows Vista, Windows Server 2008, Windows XP with SP2, Windows XP with SP3, Windows Server 2003 with SP1, and Windows Server 2003 with SP2. Windows Firewall drops incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). Windows Firewall provides a level of protection from malicious users and programs that rely on unsolicited incoming traffic to attack computers. In Windows Vista and Windows Server 2008, Windows Firewall can also drop outgoing traffic.

Windows Firewall with Advanced Security allows you to block incoming and outgoing connections based on settings that you configure through a Microsoft Management Control (MMC) snap-in. This snap-in not only provides an interface for configuring Windows Firewall locally, but also for configuring Windows Firewall on remote computers and by using Group Policy. Firewall functions are now integrated with Internet Protocol security (IPsec) protection settings, which reduces the possibility of conflict between the two protection mechanisms. Windows Firewall with Advanced Security supports separate profiles for when computers are domain-joined or connected to a private or public network. It also supports the creation of rules for enforcing server and domain isolation policies. Windows Firewall with Advanced Security supports more precise rules, including Active Directory users and groups, source and destination IP addresses, IP port number, ICMP settings, IPsec settings, specific types of interfaces, services, and more.

For more information, see the [Windows Firewall](http://technet.microsoft.com/en-us/network/bb545423.aspx) page on TechNet.

* **Microsoft Forefront Internet Security and Acceleration Server**. Microsoft Forefront™ Internet Security and Acceleration (ISA) Server can help you secure your network in several ways. For example, you can use it to allow users to remotely access your organization's applications over the Internet. To provide this access, you can configure ISA Server to pre-authenticate incoming user requests, inspect all traffic at the application layer (including encrypted traffic), and provide automated publishing tools. In addition, if your organization includes branch offices, ISA Server allows you to use HTTP compression, content caching, and virtual private network (VPN) capabilities to make expanding your network easy and secure. ISA Server can also help you protect your network from both internal and external Internet-based threats through its proxy-firewall architecture, content inspection capabilities, detailed policy settings, and comprehensive alerting and monitoring capabilities.

For more information, see [Forefront Edge Security TechCenter](http://technet.microsoft.com/en-us/forefront/edgesecurity/default.aspx).

* **Server and Domain Isolation Using Internet Protocol security (IPsec) and Active Directory Group Policy**. Server and domain isolation creates a layer of end-to-end protection that can greatly reduce the risk of costly malicious attacks and unauthorized access to your networked resources. Based on Windows IPsec and Active Directory Group Policy, this solution enables you to dynamically segment your Windows environment into more secure and isolated logical networks. There are different ways to create an isolated network, and this solution offers the flexibility to logically isolate an entire managed domain or create more secure virtual networks of specific servers, sensitive data, and clients, thus limiting access to only authenticated and authorized users, or requiring that specific servers or networks protect all data using encryption. By requiring data encryption for the traffic exchanged between specific network hosts or network subnets, you can satisfy business partner and regulatory requirements to encrypt data when it traverses a network.

For more information, see the [Server and Domain Isolation](http://technet.microsoft.com/en-us/network/bb545651.aspx) page on TechNet.

* **Windows Server 2003 and Windows Server 2008 Security Configuration Wizard**. The Security Configuration Wizard can help you secure your network by reducing the attack surface on servers running Windows Server 2003 with SP2 or Windows Server 2008. The Security Configuration Wizard determines the minimum functionality required for a server's roles and disables functionality that is not required. Specifically, the Security Configuration Wizard performs the following tasks:
* Disables unneeded services.
* Blocks unused ports.
* Allows further address or security restrictions for ports that are left open.
* Prohibits unnecessary IIS Web extensions, if applicable.
* Reduces protocol exposure within server message blocks (SMBs), LanMan, and Lightweight Directory Access Protocol (LDAP).
* Defines a high signal-to-noise audit policy.

The Security Configuration Wizard can guide IT professionals through the process of creating, editing, applying, or rolling back a security policy based on the selected roles of the server. The security policies that are created with SCW are XML files that when applied, configure services, network security, specific registry values, audit policy, and IIS, if applicable.

For more information, see [Security Configuration Wizard for Windows Server 2003](http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.mspx). For information about enhancements to the Security Configuration Wizard in Windows Server 2008, download the wizard from [Windows Server 2008 Security Configuration Wizard and SC Configuration Manager 2007 Service Pack 1](http://www.microsoft.com/downloads/details.aspx?familyid=8A08A66B-EA5B-423F-9C5D-04205F5A25EF).

* **Remote Desktop Connection Using Server Authentication**. Remote Desktop Connections are a powerful way to allow users to access shared client computers and servers. This technology can be a cost-effective way to create shared development and testing computers. In addition, you can use these computers as central access points for many types of projects and allow users from outside your network to access them, thereby isolating the risks they pose to network security. Also, the Remote Desktop Connection 6.0 client update enables IT professionals to configure server authentication. With server authentication, you can prevent users from connecting to a different computer or server than they intended, which could potentially expose confidential information. Microsoft introduced this feature in Windows Vista and in Windows Server 2008. Computers running Windows Server 2003 with SP1 or Windows XP with SP2 can use the Remote Desktop Connection 6.0 client. The client can connect to legacy terminal servers or remote desktops as before, but server authentication only occurs when the remote computer is running Windows Vista or Windows Server 2008.

For more information, see the [Remote Desktop Connection (Terminal Services Client 6.0)](http://support.microsoft.com/kb/925876) page on the Microsoft Help and Support Web site.

* **Wi-Fi Protected Access 2**. If your organization uses a wireless network, consider upgrading to wireless routers, access points, and other devices that support the Wi-Fi Protected Access 2 (WPA2) product certification. WPA2 is a product certification available through the Wi-Fi Alliance that certifies wireless equipment as compatible with the IEEE 802.11i standard. The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA. For example, WPA2 requires support for both TKIP and AES encryption.

WPA2 is available in two different modes:

* WPA2-Enterprise uses 802.1X authentication and is designed for medium and large infrastructure mode networks.
* WPA2-Personal uses a PSK for authentication and is designed for SOHO infrastructure mode networks.

WPA2 is supported on Windows XP with SP2, Windows Vista, and Windows Server 2008. For more information, see [Wireless LAN Technologies and Microsoft Windows](http://www.microsoft.com/technet/network/wifi/wrlsxp.mspx) and the [Wi-Fi Protected Access 2 (WPA2) Overview](http://technet.microsoft.com/en-us/library/bb878054.aspx) on TechNet.

* **Network Access Protection**. Network Access Protection (NAP) is a platform for Windows Server 2008 and Windows Vista. It provides policy enforcement components that help ensure that computers connecting to a network or communicating on a network meet administrator-defined requirements for system health. Your organization can use a combination of policy validation and network access limitation components to control network access or communication. You can also choose to temporarily limit the access of computers that do not meet requirements for a restricted network. Depending on the configuration you choose, the restricted network might contain resources that are required to update the computers so that they can meet the health requirements for network access and normal communication. NAP includes an application programming interface (API) set for developers and vendors to create complete solutions for health policy validation, network access limitation, and ongoing health compliance. NAP provides limited access enforcement components for IPsec, IEEE 802.1X authenticated network connections, VPNs, and DHCP. You can use these technologies together or separately. With these capabilities, NAP can be a powerful tool to help you ensure the health and security of your network.

For more information, see [Network Access Protection](http://technet.microsoft.com/en-us/network/bb545879.aspx) on Technet.

* **Microsoft Hyper-V Server™** **Server 2008**. Microsoft Hyper-V Server 2008 Server provides a simplified, reliable, and optimized virtualization solution, enabling improved server utilization and reduced costs. Because Hyper-V Server is a dedicated stand-alone product, which contains only the Windows Hypervisor, Windows Server driver model, and virtualization components, it provides a small footprint and minimal overhead. Hyper-V Server easily plugs into customers’ existing IT environments, enabling them to take advantage of their existing patching, provisioning, management, support tools, processes, and skills. Hyper-V Server allows your organization to run multiple operating systems on one computer that can help you meet PCI DSS requirement 2.2.1, which mandates that your organization run only one major function per server. For example, you can use Hyper-V Server to deploy a virtual Web server, a virtual database server, and a virtual file server on the same computer.

Microsoft Hyper-V Server 2008 is available as a free download from Microsoft. For more information, see [Microsoft Hyper-V Server 2008 Server](http://technet.microsoft.com/en-us/library/cc732470.aspx) on Technet.

## Host Control

Host control solutions control the operating systems in servers and workstations. They also implement security best practices at all levels of the operating system in each host, maintain the most current updates and hotfixes, and use secure methods for daily operations.

### PCI DSS Requirements Automated

Host control solutions can help you address PCI DSS requirements by keeping operating systems current and securely configured. Specifically, host control can help you comply with PCI DSS requirements 6 and 11.

For the full text of each of these requirements, see the [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers a number of technologies that you can use together and independently to create host control solutions. As with other technology solutions, design these solutions to meet PCI DSS requirements, as well as any other regulatory requirements that are applicable to your organization.

* **Microsoft Security Assessement Tool (MSAT)**. A free tool that provides organization with the ability to assess weaknesses in a working IT environment. MSAT provides guidance, reveals a prioritized list of issues, and helps provide specific guidance to minimize those risks. MSAT is an easy, cost-effective way to start strengthening the security of your computing environment and your business. Start the process by taking a snapshot of your current security state, and then use MSAT to continuously monitor your infrastructure’s ability to respond to security threats. MSAT consists of over 200 questions covering infrastructure, applications, operations, and people. For more information about the MSAT tool, see the [Microsoft Security Assessement Tool](http://technet.microsoft.com/en-us/security/cc185712.aspx) page on TechNet.
* **Microsoft Baseline Security Analyzer (MBSA)**. One of the primary tools you can use to assess risk to cardholder data in your organization is the MBSA tool. This easy-to-use tool identifies common security misconfigurations in a number of Microsoft products, including the Windows operating system, Internet Information Services, SQL Server, Internet Explorer, and Microsoft Office. The MBSA tool also scans for missing security updates, update rollups, and service packs published to Microsoft Update. You can run the MBSA tool from the command prompt or from a GUI, and you can use it with Microsoft Update and Windows Server Update Services. Because keeping your systems updated is a very important way to make cardholder data as secure as possible, the MBSA tool can be an invaluable tool in assessing data risk in your organization.

For more information, see [Microsoft Baseline Security Analyzer](http://go.microsoft.com/fwlink/?LinkId=8560) on TechNet.

* **Microsoft Windows Server Update Services**. Microsoft Windows Server Update Services (WSUS) with SP1 enables your organization to deploy many of the latest Microsoft product updates published to the Microsoft Update site. WSUS is an update component of Windows Server that offers an effective and quick way to help keep systems updated. WSUS provides a management infrastructure that consists of the following components:
* **Microsoft Update**. The Microsoft Web site that WSUS components connect to for Microsoft product updates.
* **Windows Server Update Services server**. The server component that installs on computers inside the organization's firewall that are running Microsoft Windows 2000 Server SP4 or Windows Server 2003. WSUS server provides features that administrators need to manage, and distributes updates through a Web-based tool, which they can access from Internet Explorer on any Windows computer in the organization's network. In addition, a WSUS server can be the update source for other WSUS servers.
* **Automatic Updates**. The client computer component built into Windows Vista, Windows Server 2003, Windows XP, and Windows 2000 SP3. With Automatic Updates, both server and client computers can receive updates from Microsoft Update or from a server running WSUS.

These services help you to keep all host environments on your network updated with the latest security fixes from Microsoft for the products installed on a specific host.

For more information, see [Microsoft Windows Server Update Services](http://go.microsoft.com/fwlink/?LinkId=71054) on TechNet.

* **Microsoft System Center Configuration Manager**. If your organization uses System Center Configuration Manger 2007 to manage client computers and servers, you might already have some of the tools you need to perform risk assessment for cardholder data. With Configuration Manger 2007, your organization can remotely manage security settings on computers running Windows operating systems over distributed networks. You can inventory computers on your network, determine whether they have installed required software updates, and track the progress of update rollouts to those computers. Configuration Manger also enables you to generate reports that identify your hardware and software inventory, the configuration details and status of the computers on your network, and the status of software deployments and deployment errors. These Configuration Manger features can be very important in assessing risk to cardholder data within your organization.

For more information about Configuration Manger, see the [Microsoft System Center Configuration Manager](http://www.microsoft.com/systemcenter/configurationmanager/en/us/default.aspx) home page.

* **Security Compliance Management Toolkit Series**. The toolkit series offers DCM Configuration Packs that provide security baselines for Windows Server 2008, Windows Server 2003, Windows Vista, Windows XP, and Microsoft Office 2007. The purpose of the toolkit series is to reduce the work required to manage DCM configuration baselines that maintain recommended security settings for different operating systems from Microsoft. For more information about how to establish security baselines for Microsoft products in your environment, see the guidance provided in each toolkit of the series.
* **Microsoft Desktop Optimization Pack for Software Assurance**. The Microsoft Desktop Optimization Pack for Software Assurance is a subscription service that reduces application deployment costs, enables delivery of applications as services, and provides better management and control of enterprise desktop environments. The desktop optimization pack is an effective host control solution that enables you to achieve the following:
* Streamline and accelerate the application management life cycle from planning and predictable deployment, to using, maintaining, and migrating software.
* Enhance the management of your organization’s software assets.
* Accelerate and simplify desktop deployments and migrations.

The Microsoft Desktop Optimization Pack is available only to customers with Software Assurance coverage on their desktops. For more information, see [Optimizing the Windows Desktop](http://www.microsoft.com/windows/products/windowsvista/buyorupgrade/optimizeddesktop.mspx).

For links to specific host security guidelines and procedures for many Microsoft products, see the [Learning Resources for Solution Accelerators](http://technet.microsoft.com/en-us/solutionaccelerators/bb899722.aspx) page on TechNet..

## Malicious Software Prevention

Malicious software prevention solutions are key elements in keeping cardholder data secure across your network. By preventing spam and keeping systems on the network free of viruses and spyware, these solutions can help ensure that systems across your network are working at their peak and that sensitive data is not transmitted unintentionally to unauthorized parties.

### PCI DSS Requirements Automated

The malicious software prevention solutions that you choose can help your organization meet PCI DSS requirements 5 and 6.

For the full text of each of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers a number of technologies that you can use together and independently for malicious software prevention. Consider these technologies in the context of your larger PCI DSS compliance efforts, as well as any broader regulatory requirements for your organization.

* **Microsoft Forefront**. Forefront is a suite of security products that provide protection for client operating systems, application servers, and the network edge. You can use Forefront with your existing IT infrastructure to protect your servers and client computers from malware and other malicious attacks that originate inside or outside of your organization.

In particular, Forefront Client Security provides protection from malicious software for clients across an organization, There are two parts to the Forefront Client Security solution. One part is the Security Agent—installed on business desktop, laptop, and server operating systems—that provides real-time protection and scheduled scanning of threats such as spyware, viruses, and rootkits. The other part is the central management server, which enables administrators to easily manage and update preconfigured or customized malware protection agents, and generate reports and alerts about the security status of their environment.

For more information, see the [Microsoft forefront](http://www.microsoft.com/forefront/default.mspx) home page.

* **The Microsoft Windows Malicious Software Removal Tool** checks computers running Windows Vista, Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from Microsoft Update, Windows Update and the Microsoft Download Center.

For more information, see the [Malicious Software Removal Tool](http://www.microsoft.com/security/malwareremove/default.mspx) page.

Note   Windows Defender and the Malicious Software Removal Tool can also help you discover whether a malicious program uses a rootkit. Rootkits are mechanisms that malicious software creators use to hide their presence from spyware blockers as well as antivirus and system management utilities. For more information about rootkits and how to detect them, see the [Rootkit Revealer](http://www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx) page on TechNet.

* **Third-Party Filters with Microsoft Forefront ISA Server**. In addition to providing network security solutions, ISA Server can help protect your organization from malware attacks. You can do this by using custom or third-party filters that remove malware before it reaches your corporate network.

For more information, see the [Internet Security and Acceleration Server](http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/default.aspx) home page.

## Application Security

To address PCI DSS requirements, Microsoft recommends to consider your application security solutions on two fronts. First, require that any new applications created by developers within your organization comply with secure development practices. Second, ensure that you use the security guidelines supplied with any software applications that you purchase from Microsoft or any third-party supplier.

### PCI DSS Requirements Automated

Developing and maintaining secure applications, whether they are Web or Windows–based, is an important step in your PCI DSS compliance efforts. In particular, these technology solutions allow you to meet requirement 6.

For the full text of this requirement, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers specific guidance and tools for developing secure applications. It also offers the following specific guidelines for using its primary server products securely:

* **Microsoft Visual Studio®** **2008**. [Visual Studio](http://msdn.microsoft.com/en-us/vstudio/default.aspx) supplies a number of tools that enable developers to check their code for security violations as they develop it, including the following:
* Code Analysis for Managed Code checks .NET code for vulnerabilities, including security vulnerabilities.
* Code Analysis for C and C++ is a static analysis tool that can help developers find a variety of security issues.
* Standard Annotation Language can help developers find security vulnerabilities that might not be picked up by the C or C++ code compilers.
* When compiling unmanaged code written in C or C++, developers should always compile with the /GS stack overrun detection capability and link the code with the /SafeESH option.
* RPC developers should compile their code with the MIDL /robust flag specified.

The Microsoft Security Development Lifecycle suggests to use such tools as FxCop, PREfast, and the GS C++ compiler option to ensure that code runs without compromising known security issues.

For more information, see [Patterns and Practices Security Guidance](http://msdn.microsoft.com/en-us/library/ms998408.aspx) and [Writing Quality Code](http://msdn.microsoft.com/en-us/library/4dtdybt8.aspx) on MSDN.

* + - **Microsoft Intelligent Application Gateway (IAG) 2007**. A part of Microsoft Forefront Network Edge Security, IAG provides a secure socket layer (SSL) VPN, a Web application firewall, and endpoint security management that enable access control, authorization, and content inspection for a wide variety of line-of-business applications. Together these technologies provide mobile and remote workers with easy and flexible secure access from a broad range of devices and locations, including kiosks, desktop computers, and mobile devices. IAG also enables IT administrators to enforce compliance with application and information usage guidelines through a customized remote access policy based on device, user, application, or other business criteria. Key benefits include:
* A unique combination of SSL VPN–based access, integrated application protection, and endpoint security management.
* A powerful, Web application firewall that helps keep malicious traffic out and sensitive information in.
* Reduced complexity of managing secure access and protecting business assets with a comprehensive, easy-to-use platform.
* Interoperability with core Microsoft application infrastructure, third-party enterprise systems, and custom in-house tools.

For more information, see the [Intelligent Application Gateway Overview](http://www.microsoft.com/forefront/edgesecurity/iag/overview.mspx).

#### Guidelines

Microsoft offers the following guidelines to help ensure the security of your applications:

* **Security Development Lifecycle**. Organizations that develop custom software solutions to handle cardholder data should consider implementing the Microsoft Security Development Lifecycle (SDL). The SDL introduces security and privacy early and throughout the development process. Combining a holistic and practical approach, the SDL is risk-based with the goal of protecting users by reducing the number and severity of vulnerabilities in code. The SDL starts with planning for secure applications, ensures the use of secure coding techniques, and includes testing and deploying applications securely after development is complete.

For more information, see [The Microsoft Secure Development Lifecycle](http://go.microsoft.com/?linkid=8941316).

* **Microsoft Operations Framework (MOF) 4.0**. MOF delivers practical guidance for everyday IT practices and activities, helping users establish and implement reliable, cost-effective IT services. It encompasses the entire IT life cycle through a defined management layer, phases, and service management functions.
* **Follow Product Security Guidelines**. Microsoft offers security guidelines for a number of its software products. Of particular interest to large and medium-sized organizations are security guidelines for Exchange Server, Systems Management Server, and SQL Server. For more information on security guidelines for these products, see the "Application Security" section of the [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419).

## Messaging and Collaboration

To address PCI DSS requirements, you must ensure that the messaging and collaboration software your organization uses is configured and set up securely. Because messaging and collaboration applications have become essential tools in the payment card industry, it is vital to do all you can to ensure that any documents or e-mail messages that might contain cardholder data are secure.

### PCI DSS Requirements Automated

Common methods to help prevent messaging security breaches include messaging gateways, secure messaging servers, and messaging content filtration. Both messaging gateways and messaging content filtration route messages to a specialized software application, which can use a variety of methods to isolate specific word strings, number strings, word patterns, or other items, depending on how the solution was designed. Messages that contain these key words or strings can then be placed in quarantine until the suspect information they contain is checked, or the solution can simply delete and purge the messages. These methods can help you secure cardholder data when it is sent through an e-mail message or document in a collaboration environment. All of these techniques and solutions can help you address PCI DSS requirement 4.

For the full text of this requirement, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft provides a number of solutions that can help you secure messaging and collaboration software. Ensure to deploy each in an organized way so that as few security vulnerabilities as possible remain after you have finished. Each solution addresses different organizational needs:

* **Microsoft Exchange Server**. As with document management, Exchange can help you define powerful solutions for your organization’s messaging needs while keeping any cardholder data in e-mail messages secure. Exchange Server 2007 includes unified messaging, which consolidates incoming e-mail, voice mail, and faxes into a single inbox. It also offers features that enable your organization to apply retention rules, scan and act on messages in transport, flexibly journal, and perform rich text searches across all deployed mailboxes.

For more information, see the [Microsoft Exchange Server](http://www.microsoft.com/exchange/default.mspx) Web site.

* **Microsoft Forefront Security for Exchange Server**. Microsoft Forefront Security for Exchange Server helps protect your e-mail infrastructure from infection and downtime through an approach that emphasizes layered defenses, optimization of Exchange Server performance and availability, and simplified management control.
* **Comprehensive Protection**. Microsoft Forefront Security for Exchange Server includes multiple scan engines from industry-leading security firms integrated in a single solution to help businesses protect their Exchange messaging environments from viruses, worms, and spam.
* **Optimized Performance**. Through deep integration with Exchange Server, scanning innovations and performance controls, Forefront Security for Exchange Server helps protect messaging environments while maintaining uptime and optimizing server performance.
* **Simplified Management**. Forefront Security for Exchange Server also enables administrators to easily manage configuration and operation, automated scan engine signature updates, and reporting at the server and enterprise level.

For more information, see the [Microsoft Forefront](http://www.microsoft.com/forefront/default.mspx) home page.

* **Microsoft Exchange Hosted Services**. Microsoft Exchange Hosted Services for messaging security and management is composed of four distinct services that help organizations protect themselves from e-mail-borne malware, satisfy retention requirements for compliance, encrypt data to preserve confidentiality, and preserve access to e-mail during and after emergency situations. The services are deployed over the Internet using a Software as a Service model that helps minimize additional capital investment, free up IT resources to focus on other value-producing initiatives, and mitigate messaging risks before they reach the organization's firewall.

For more information, see the [Microsoft Exchange Hosted Services](http://www.microsoft.com/exchange/services/default.mspx) home page.

* **Microsoft Office Information Rights Management (IRM)**. Office is the premier suite of productivity applications for organizations. The IRM feature of Microsoft Office can help your organization control access to sensitive information such as cardholder data.

Specifically, the Office IRM feature helps your organization accomplish the following:

* Prevent authorized recipients of protected information from forwarding, copying, modifying, printing, faxing, or cutting and pasting information for unauthorized use.
* Prevent protected information from being copied with the Microsoft Windows Print Screen function.
* Provide information with the same level of protection wherever it goes, which is referred to as *persistent protection*.
* Provide the same level of protection to e-mail attachments, as long as the attachments are files created with other Office programs, such as Excel or Word.
* Protect information in e-mail messages or documents that have been set to expire, so that the information can no longer be viewed after a specified period of time.
* Enforce policies that govern the use and dissemination of information within and outside the organization.

Office IRM is built on the Microsoft Windows Rights Management Services platform. To enable this feature in Office, you must purchase RMS server licenses.

For more information, see the [About Information Rights Management](http://office.microsoft.com/en-us/help/HP062208591033.aspx) page of the Microsoft Office Web site.

* **Microsoft Windows SharePoint Services** **Information Rights Management (IRM)**. As with your document management solutions, SharePoint Services IRM can help you make your collaboration solutions address PCI DSS requirements. This technology allows you to create a persistent set of access controls that are attached to the content rather than a specific network location, which helps you control access to files even after they leave your direct control. IRM is available for files that are located in document libraries and stored as attachments to list items. Site administrators can elect to protect downloads in a document library with IRM. When a user attempts to download a file from the library, Windows SharePoint Services verifies that the user has permissions to the file, and then issues a license to the user that enables access to the file at the appropriate permissions level. Windows SharePoint Services then downloads the file to the user's computer in an encrypted, rights-managed file format.

Office IRM is built on the Microsoft Windows Rights Management Services platform. To enable this feature in Office, you must purchase RMS server licenses.

For more information, see [Information Rights Management in Windows SharePoint Services Overview](http://msdn.microsoft.com/en-us/library/ms458245.aspx) page on MSDN.

## Data Classification and Protection

Data classification and protection solutions are central elements in efforts to successfully address PCI DSS requirements and keep cardholder data secure. These solutions deal with how to apply security classification levels to cardholder data either on a system or in transmission. This solution category also deals with data protection in terms of providing confidentiality and integrity to data that is either in storage or in transmission. Cryptographic solutions are the most common method that organizations use to provide data protection.

### PCI DSS Requirements Automated

Data classification and protection solutions help you meet PCI DSS requirements by securing cardholder data when it is stored in a database, transmitted from one server to another, or transmitted into your network when a cardholder makes a purchase. Using these solutions helps you address PCI DSS requirements 3, 4 and 7.

For the full text of each of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers a number of technologies that can help you classify and protect cardholder data, whether it is transmitted over your network, stored in a document on an employee’s computer, or stored to a database. These technologies include the following:

* **BitLocker™ Drive Encryption**. BitLocker Drive Encryption helps you protect cardholder data by providing drive encryption and integrity checking on early-boot components. Drive encryption protects data by preventing unauthorized users from breaking Windows file and system protection on lost or stolen computers. This protection is achieved by encrypting the entire Windows volume. With BitLocker, all user and system files are encrypted, including the swap and hibernation files. Integrity checking the early-boot components help to ensure that data decryption is performed only if those components appear unmolested and that the encrypted drive is located in the original computer. BitLocker is available in Windows Vista Enterprise and Ultimate and Windows Server 2008.

For more information, see the [BitLocker Drive Encryption](http://technet.microsoft.com/en-us/windows/aa905065.aspx) page on TechNet.

* **Windows Encrypting File System (EFS)**. EFS provides the core file encryption technology used to store encrypted files on NTFS file system volumes. After you encrypt a file or folder, you work with the encrypted file or folder just as you do with any other files and folders.

Encryption is transparent to the user that encrypted the file, which means that they do not have to manually decrypt an encrypted file before they can use it. Users can open and change the file as they typically do.

Using EFS is similar to using permissions on files and folders. You can use both methods to restrict access to data. However, an intruder who gains unauthorized physical access to your encrypted files or folders will be prevented from reading them. An intruder who tries to open or copy your encrypted file or folder receives an access-denied message. Permissions on files and folders do not protect against unauthorized physical attacks.

For more information, see the [Encrypting File System](http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx) page on the Windows Vista Web site.

* **Microsoft Windows Rights Management Services**. Microsoft Windows Rights Management Services (RMS) is a software platform that helps applications safeguard cardholder data from unauthorized use—both online and offline, inside and outside of the firewall.

RMS augments an organization's security strategy by protecting information through persistent usage policies, which remain with the information no matter where it goes. RMS–enabled applications can be used to manage, control, and audit access to documents that contain cardholder information. For other Windows versions, the RMS client is available as a free download.

For more information, see [Windows Rights Management Services.](http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx)

* **Microsoft SQL Server® 2008 Encryption and Key management**. When you store cardholder data in SQL Server, you can implement one of three built-in capabilities in SQL Server 2008 to protect cardholder data:
* SQL Server 2008 Transparent Data Encryption (TDE) offers full data encryption. TDE encrypts all database files including data files, log files, and backup files.
* SQL Server 2008 cell level encryption offers encryption of individual columns and cells. The use of cell level encryption requires modifications to client applications to handle the explicit encryption.
* **SQL Server 2008 Extensible Key Management (EKM)** offers split encryption key ownership. EKM provides a robust key management solution that ensures you can encrypt all data using TDE. EKM reduces issues with managing a potentially complex key management solution in SQL Server.

For more information, see the [Microsoft SQL Server 2008](http://go.microsoft.com/fwlink/?LinkId=146989) Web site, or [Deploying SQL Server 2008 Based on Payment Card Industry Data Security Standards (PCI DSS)](http://www.parentenet.com/whitepapers/SQL2008_PCI.pdf) (PDF) by Parente Randolph.

## Identity Management

Identity management is another important element in achieving PCI DSS compliance. Identity management solutions allow you to limit the personnel who can access, process, and transmit cardholder data. Your organization can use these identity management solutions to help manage digital identities and permissions for your employees, clients, and partners.

### PCI DSS Requirements Automated

Using identity management solutions can allow you to address PCI DSS requirement 8 by helping you create and assign a unique ID to each person in your organization that has access to a computer. These solutions can also help you restrict access to cardholder data based on that unique ID, the principle of PCI DSS requirement 7.

For the full text of this requirement, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft provides the following technologies to help you address your organization’s identity management requirements:

* **Active Directory Domain Services**. Active Directory Domain Services (AD DS) supports a number of techniques to help you control the personnel who can access cardholder data on your network and outside of it. AD DS supports Kerberos authentication, one of the default Windows Authentication techniques. Kerberos provides secure user authentication with an industry standard that permits interoperability. The AD DS domain controller maintains user account and login information to support the Kerberos service. In addition, AD DS supports smart card authentication. You can require remote users or administrators of systems that contain cardholder data to use a smart card and PIN to access your network. AD DS also supports credential roaming, a service that enables users who have to use multiple computers to use the same credentials on each of those computers. And AD DS allows your organization to customize the credential providers that it uses to authenticate users. These features can help you precisely control how you allow AD DS accounts to access cardholder data, and which accounts you provide with access to that data.

For more information, see the [Active Directory Domain Services](http://technet.microsoft.com/en-us/library/cc770946.aspx) page on TechNet.

* **Microsoft Active Directory Federation Services**. With Active Directory Federation Services (ADFS), you can create identity management solutions that extend beyond the traditional boundaries of your Active Directory forest. By employing ADFS, your organization can extend its existing AD DS infrastructure to provide access to resources that are offered by trusted partners across the Internet. These trusted partners can include external third parties or other departments or subsidiaries in the same organization.

ADFS is tightly integrated with AD DS. ADFS retrieves user attributes from AD DS and it authenticates users by using AD DS. ADFS also uses Windows Integrated Authentication. ADFS is available in Windows Server 2003 R2 and Windows Server 2008.

For more information, see [Overview of Active Directory Federation Services (ADFS) in Windows Server 2003 R2](http://www.microsoft.com/WindowsServer2003/R2/Identity_Management/ADFSwhitepaper.mspx).

* **Microsoft Identity Lifecycle Manager**. Microsoft Identity Lifecycle Manager (ILM) simplifies the process of matching and managing identity records from disparate data repositories and helps prevent anomalies, such as active records for employees who have left the organization. ILM provides your organization with a policy framework to control and track the identity and access data that helps manage compliance. It also includes self-help tools for users, enabling your IT department to improve efficiency by securely delegating many tasks to users. Another key feature of ILM is that it includes a Windows–based certificate management solution that integrates with the Windows Server 2008 operating system and Active Directory to provide a turnkey solution for managing the end-to-end life cycle of smart cards and digital certificates for the Windows Server 2008 Certification Authority.

ILM enables your organization to accomplish the following:

* Synchronize identity information across a variety of heterogeneous directory and nondirectory identity stores. This capability enables you to automate the process of updating identity information across disparate platforms while maintaining the integrity and ownership of that data across the organization.
* Provision and deprovision user accounts and identity information such as distribution, e-mail accounts, and security groups across systems and platforms. You can create new accounts for employees quickly based on events or changes in authoritative stores such as the human resources system. In addition, when employees leave an organization, you can immediately deprovision them from the same systems.
* Manage certificates and smart cards. ILM includes a workflow and policy–based solution that enables organizations to easily manage the life cycle of digital certificates and smart cards. ILM leverages Active Directory Domain Services and Active Directory Certificate Services to provision digital certificates and smart cards with automated workflow to manage the entire life cycle of certificate–based credentials. ILM significantly lowers the costs associated with digital certificates and smart cards by enabling organizations to more efficiently deploy, manage, and maintain a certificate-based infrastructure. It also streamlines the provisioning, configuration, and management of digital certificates and smart cards, while increasing security through strong, multifactor authentication technology.

For more information, see the [Microsoft Identity Lifecycle Manager 2007 FP1](http://www.microsoft.com/windowsserver/ilm2007/default.mspx) home page.

* **Microsoft SQL Server 2008**. You can use SQL Server in conjunction with other technologies to create identity management solutions. For example, you can use SQL Server 2008 extensible key management (EKM) and transparent data encryption (TDE)to store username and password information and to map certificates to user accounts and other solutions. You can user SQL Server in concert with Microsoft ILM, Active Directory Domain Services, Group Policy, and ACLs to restrict users’ access to cardholder data stored in another database, in documents, or in directories.

For more information, see the [Microsoft SQL Server 2008](http://www.microsoft.com/sql/default.mspx) Web site or [Deploying SQL Server 2008 Based on Payment Card Industry Data Security Standards (PCI DSS)](http://www.parentenet.com/whitepapers/SQL2008_PCI.pdf) (PDF) by Parente Randolph.

#### Operating System Support Features

* **Public Key Infrastructure**. A public key infrastructure (PKI) is a system of digital certificates, certification authorities (CAs), and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction through the use of public key cryptography. This infrastructure can allow you to secure and exchange cardholder data with strong security across the Internet, extranets, intranets, and applications.

PKI support is available in Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Vista, and Windows XP Professional.

For more information, see [Public Key Infrastructure for Windows Server 2003](http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx).

## Authentication, Authorization, and Access Control

Authentication is the process of identifying users. In IT environments, authentication usually involves usernames and passwords, but it can include methods to demonstrate identity, such as smart cards, retina scans, voice recognition, or fingerprints. Authorization focuses on determining whether the authenticated identity is allowed to access requested resources. You can choose to grant or deny access based many criteria, such as the network address of the client, the time of day, or the user's browser.

When planning your authentication, authorization, and access control strategy, Microsoft also recommends to develop a strategy for granting user account permissions to all resources across your network. For more information, see [Applying the Principle of Least Privilege to User Accounts on Windows XP](http://technet.microsoft.com/en-us/library/bb456992.aspx), [Inside Windows Vista User Account Control](http://technet.microsoft.com/en-us/magazine/cc138019.aspx), and [Configuring Applications for Least Privilege](http://technet.microsoft.com/en-us/library/dd163542.aspx). on Microsoft TechNet.

### PCI DSS Requirements Automated

Authentication, authorization, and access control are key portions of your cardholder data security strategy, particularly in combination with data classification and protection, and identity management solutions. In this context, authentication, authorization and access control solutions can help your organization meet PCI DSS requirements 6, 7, and 8.

For the full text of each of these requirements, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers several technologies to help you create and integrate authentication, authorization, and access control strategies into your PDI DSS compliance solution:

* **Active Directory Domain Services**. Much of Active Directory Domain Services (AD DS) in Windows 2000 Server, Windows Server 2003, and Windows Server 2008 focuses on authentication, authorization, and access control. For example, AD DS supports Kerberos authentication, one of the default Windows Authentication techniques. Kerberos provides secure user authentication with an industry standard that permits interoperability. The AD DS domain controller maintains user account and login information to support the Kerberos service. AD DS also supports smart card authentication. You can require remote users or administrators of systems containing cardholder data to use a smart card and PIN to access your network. AD DS supports credential roaming, a service which enables users who have to use multiple computers to use the same credentials on each of those computers. With AD DS, your organization can also customize the credential providers that it uses to authenticate users. AD DS also allows you to delegate administrative tasks. These features can help you precisely control how you allow AD DS accounts to access cardholder data, and to which accounts you provide access to that data.

For more information, see the [Active Directory Domain Services](http://technet.microsoft.com/en-us/library/cc770946.aspx) page on TechNet.

* **Windows CardSpace**. The Internet continues to be increasingly valuable, and yet also faces significant challenges. Online identity theft, fraud, and privacy concerns are rising. Users must track a growing number of accounts and passwords. This burden results in "password fatigue," which results in nonsecure practices, such as reusing the same account names and passwords at many sites. Many of these problems are rooted in the lack of a widely adopted identity solution for the Internet.

CardSpace is the Microsoft implementation of an Identity Metasystem that enables users to choose from a portfolio of identities that belong to them, and then use them in contexts where they are accepted, independent of the underlying identity systems where the identities originate and are used.

For more information, see the [Windows CardSpace](http://msdn.microsoft.com/en-ca/library/ms733090.aspx) section on MSDN.

* **Microsoft Internet Authentication Service**. Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and VPN connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. By doing this, IAS performs authentication steps for remote connections before they reach your organization’s network. With the credentials that users supplied to connect remotely, you can authorize them to access only those resources on your network that they need to accomplish their work.

For more information, see the [Internet Authentication Service](http://technet.microsoft.com/en-us/network/bb643123.aspx) page on TechNet.

#### Operating System Support Features

* **Using Access Control Lists to Grant Resource Permissions**. An access control list (ACL) is a mechanism used by operating systems since Microsoft Windows NT to protect resources such as files and folders. ACLs contain multiple access control entries (ACEs) that associate a principal (usually a user account or group of accounts) with a rule that governs the use of the resource. ACLs and ACEs let your organization allow or deny rights to resources based on permissions that you can associate with user accounts. For example, you can create an ACE and apply it to the ACL of a file to bar anyone but an administrator from reading the file. You must use this technology within your larger identity management solution, but it remains a good way to restrict access to cardholder data to only those individuals with a business need.

For more information, see [How Security Descriptors and Access Control Lists Work](http://technet.microsoft.com/en-us/library/cc781716.aspx) on TechNet, and the [ACL Technology Overview](http://msdn2.microsoft.com/en-us/library/ms229742.aspx) on MSDN.

* **Windows Firewall in Windows Vista and Windows Server 2008**. As previously discussed, Windows Firewall in Windows Vista and Windows Server 2008 can help you protect your systems and networks from malicious attacks. It can also help you control which users, computers, and groups can access resources on a computer or domain. When you use Windows Firewall with Advanced Security, you can create rules that filter connections by an AD DS user, computer, or group. To create these types of rules, you must secure the connection with IPsec using credentials that carry AD DS account information, such as Kerberos version 5 protocol.

For more information, see the [Windows Firewall](http://technet.microsoft.com/en-us/network/bb545423.aspx) page on TechNet.

## Vulnerability Identification

Vulnerability identification solutions provide tools that your organization can use to help test for vulnerabilities in its information systems. Your IT personnel must be aware of vulnerabilities in the IT environment before they can effectively address them. The ability to restore data that was inadvertently lost because of user error is also involved in vulnerability identification.

### PCI DSS Requirements Automated

Vulnerability solutions allow you to meet PCI DSS requirement 11, which requires organizations to regularly testing security systems and procedures.

For the full text of this requirement, see [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF) on the PCI Security Standards Council's Web site.

### Available Technologies

Microsoft offers the following solution to help you design vulnerability identification solutions to address your PCI DSS requirements:

* **Microsoft Baseline Security Analyzer (MBSA)**. As with assessing risk when designing many of your cardholder data protection controls, the MBSA tool enables you to periodically review any vulnerability that might compromise the security of cardholder data. You can use the MBSA tool to locate common security misconfigurations in a number of Microsoft products, including the Windows operating system, Internet Information Services (IIS), SQL Server, Internet Explorer, and Microsoft Office. The MBSA tool also scans for any missing security updates, update rollups, and service packs published to Microsoft Update. You can run the tool from the command prompt or from a GUI, and you can use it with Microsoft Update and Windows Server Update Services. Because keeping your systems updated is a very important way to make cardholder data as secure as possible, the MBSA tool can be invaluable in determining whether your product installations have created cardholder data vulnerabilities over time.

For more information, see the [Microsoft Baseline Security Analyzer](http://go.microsoft.com/fwlink/?LinkId=16384) page on TechNet.

## Monitoring, Auditing, and Reporting

Monitoring and reporting solutions collect and audit logs that are generated by authentication processes and access to systems. You can design these solutions to collect specific information based on PCI DSS, or use existing logs built into operating systems or software packages.

A subcategory of monitoring and reporting is the collection, analysis, and correlation of all logged data across your organization. These actions are sometimes accomplished through a dashboard-type solution, in which you can better analyze the various information gathered throughout the organization. This type of solution allows IT management to better determine whether there are correlations between events.

### PCI DSS Requirements Automated

Monitoring, auditing, and reporting solutions can help you address PCI DSS Requirement 10, which requires organizations to track and monitor all access to network resources and cardholder data.

### Available Technologies

Microsoft offers the following technologies that allow you to monitor network access and access to cardholder data:

* **Microsoft System Center Operations Manager Audit Collection Services (ACS)**. Operations Manager 2007 can securely and efficiently extract and collect security logs from computers running Windows operating systems and store them for later analysis and reporting. The extracted logs are stored in a separate Audit Collection server database. Operations Manager ships with reporting capability that you can use for the ACS data. You can use Audit Collection to produce various compliance reports, such as supporting Sarbanes-Oxley audits. You also can use ACS for security analysis, such as intrusion detection and unauthorized access attempts.

For more information, see the [Audit Collection Services (ACS)](http://technet.microsoft.com/en-us/library/bb381258.aspx) page on TechNet.

* **Microsoft Windows Vista Event Logging Infrastructure**. Improvements to the Windows event logging infrastructure make the Windows Vista desktop easier to manage and monitor, and provide better information for troubleshooting. Strict standards ensure that events are meaningful, actionable, and well-documented. Many components that stored logging information in text files in previous versions of Windows now add events to the event log. With event forwarding, administrators can centrally manage events from computers anywhere on the network, making it easier to proactively identify problems and to correlate problems that affect multiple computers. In addition, the Event Viewer has been completely rewritten to allow users to create custom views to easily associate events with tasks, and to remotely view logs from other computers. These capabilities make it much more practical for administrators to use the event log to troubleshoot users' problems.

For more information, see the [Windows Vista Management Features](http://technet.microsoft.com/en-us/windowsvista/aa905069.aspx) page on TechNet.

* **Microsoft SQL Server2008**. SQL Server Reporting Services is a comprehensive, server-based solution that enables the creation, management, and delivery of both traditional, paper-oriented reports and interactive, Web-based reports. An integrated part of the Microsoft business intelligence framework, Reporting Services combines the data management capabilities of SQL Server and Windows Server with familiar and powerful Microsoft Office System applications to deliver real-time information to support daily operations and drive decisions. You can use these services to generate reports that analyze cardholder data and track changes to it. You can also use reporting services to more easily monitor network usage patterns and information flow.

For more information, see the [Microsoft SQL Server 2008](http://go.microsoft.com/fwlink/?LinkId=146989) Web site, or [Deploying SQL Server 2008 Based on Payment Card Industry Data Security Standards (PCI DSS)](http://www.parentenet.com/whitepapers/SQL2008_PCI.pdf) (PDF) by Parente Randolph.

#### Operating System Support Features

* **NTFS System Access Control Lists**. Your organization can use NTFS System Access Controls Lists (SACLs) on files and directories to help you track changes to files or folders on a computer. When you set a SACL on a file or folder, any actions that are performed on that file or folder are logged by the Windows operating system, which also logs who performed the action. You cannot set SACLs on computers that are formatted with the FAT file system, so your organization should use the NTFS file system format on all volumes that store user data and cardholder data.

For more information, see [User Data and Settings Management](http://technet.microsoft.com/en-us/library/bb490855.aspx) on TechNet.

## Managing PCI DSS Technology Solutions

Although using management products does not help your organization meet any specific PCI DSS requirements, they can help you keep track of the IT controls that you have implemented for compliance purposes. In creating a framework of IT controls, it is always important to be able to centrally manage those controls from as few administrators’ desks as possible.

### Available Technologies

Microsoft offers two primary tools for managing your framework of IT controls that you implement to address PCI DSS and other regulatory requirements:

* **Microsoft Forefront**. Microsoft Forefront is a suite of line-of-business security products that provide protection for client operating systems, application servers, and the network edge. You can use Forefront with your existing IT infrastructure to protect your servers and client computers from malware and other malicious attacks—all through easy integration with application servers such as Exchange, SharePoint, and Instant Messaging. Forefront also features built-in integration with Active Directory Domain Services, and uses ISA Server to work with Active Directory Domain Services (AD DS) for RADIUS, DHCP, and smart card support. Forefront also provides a centralized management tool for a central reporting location, along with a centralized location to set policy control measures.

For more information, see the [Microsoft Forefront](http://www.microsoft.com/forefront/default.mspx) home page.

* **Microsoft System Center**. Microsoft System Center is a family of management products aimed at providing the tools your organization needs to automate system management across your organization. System Center includes technologies that help automate the most common management tasks, and it also provides tools to help IT professionals detect, diagnose, and correct problems in their computing environments. Specifically, System Center provides products that perform the following functions:
* Monitor the hardware and software in a distributed environment to detect issues, and provide tools to fix those issues.
* Automate the process of installing, updating, and patching software.
* Provide implementations of standard processes for systems management.
* Handle backup and restore of Windows file server data.
* Address the monitoring and configuration requirements of smaller organizations.
* Manage virtual machines. As faster hardware lets more applications run on each machine, organizations are increasingly using virtualization to isolate those applications.
* Size installations properly by providing tools that help estimate the required resources.

For more information, see the [Microsoft System Center](http://www.microsoft.com/systemcenter/default.aspx) Web site.

# Summary

This guide provided descriptions of technology solutions that your organization can use to help achieve and maintain PCI DSS compliance. It discussed the reasons these solutions are important, and offers links to Microsoft guidance and technology that can help your organization toward achieving regulatory compliance.

The effect of implementing these solutions not only helps to provide security and compliance standards for your IT environment, but also has a positive effect on your organization's business processes. Before you implement any of the identified solutions, be sure to meet with your legal advisors and auditors to obtain legal advice about your own unique PCI DSS compliance needs, and carefully consider the impact of these solutions on the entire organization, not just in terms of compliance. Microsoft is committed to providing more in-depth research and solutions for PCI DSS and other regulatory compliance standards.

# Appendix

This appendix contains questions that are commonly asked by customers about Microsoft technology solutions and how your organization can take advantage of them to address PCI DSS requirements. It also contains a table that maps which technology solutions can help your organization address PCI DSS requirements that the guide discusses.

## Frequently Asked Questions

**Q: Why should my organization bother to comply with the Payment Card Industry Data Security Standard? Isn’t this another useless and costly standard to deal with?**

**A:** There are three reasons that your organization should work to comply with PCI DSS. One, card brands such as Visa have committed to providing financial incentives for PCI compliance and penalties for noncompliance. Two, compliance can help reduce liability in case of data loss. Three, by performing a thoughtful analysis and appropriate design of your systems, the process can actually help you better track customer data, and as a result help you to improve customer service and satisfaction.

**Q: Is Microsoft overselling its technologies for PCI DSS compliance?**

**A:** Each organization’s situation is different and this guide aims to be as comprehensive as possible. Microsoft might develop specific guidance for industry verticals. You can also contact your Microsoft sales representative for more guidance. As stated above, you can achieve better business results if you look at this not as simply a compliance project, but also as a project dedicated to improving your tracking and management of customer information.

**Q: This paper describes many technologies that organizations can use to help them comply with PCI DSS, but very few compliance solutions. Why is that?**

**A:** Each organization's situation is unique, and so it is not possible to come up with a single solution that fits all. Microsoft is committed to providing your organization with more detailed information.

**Q: What can Microsoft do to help my organization get PCI DSS certified?**

**A:** Microsoft can offer software and services that can help you address PCI DSS requirements, but it cannot ensure that your organization will achieve compliance with PCI DSS. As a vendor, we are very interested in helping your organization address these requirements, but compliance is between your organization, its auditors, and the card brands with which you work.

**Q: Doesn’t** [**PCI DSS Requirments and Security Assessment Procedures, v1.2**](https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html) **Section 3.4.1 imply that Microsoft data protection technologies cannot be used?**

**A:** No. That section says, in full:

 "If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system user accounts). Decryption keys must not be tied to user accounts."

Microsoft data protection technologies do not tie decryption keys to user accounts. For example, BitLocker Drive Encryption never ties decryption keys (PINs or recovery passwords) to user accounts in Active Directory Domain Services (AD DS). Encrypting File System (EFS) does not tie decryption keys to user accounts either. Your organization can revoke a person’s ability to decrypt a document without changing system access privileges. In certain configurations, EFS attempts to optimize the user experience by automatically placing some decryption keys in the user profiles of specific users. However, this functionality can be changed through appropriate configuration.

Table 1. PCI DSS Requirements and Associated Technology Solutions

| **Requirements** | **Technology solution sections** |
| --- | --- |
| Requirement 1 | Risk Assessment; Network Security |
| Requirement 2 | Network Security |
| Requirement 3 | Document Management; Risk Assessment; Data Classification and Protection |
| Requirement 4 | Risk Assessment; Messaging and Collaboration; Data Classification and Protection; Network Security |
| Requirement 5 | Risk Assessment; Malicious Software Prevention |
| Requirement 6 | Document Management; Risk Assessment; Change Management; Host Control; Malicious Software Prevention; Application Security; Authentication, Authorization, and Access Control |
| Requirement 7 | Document Management; Risk Assessment; Identity Management; Authentication, Authorization, and Access Control; Data Classification and Protection |
| Requirement 8 | Risk Assessment; Authentication, Authorization, and Access Control |
| Requirement 9 | Document Management |
| Requirement 10 | Document Management; Change Management; Monitoring, Auditing, and Reporting; Network Security |
| Requirement 11 | Risk Assessment; Host Control; Vulnerability Identification |
| Requirement 12 | Document Management |

## Additional Resources

This guide includes the following additional resources:

* [Applying the Principle of Least Privilege to User Accounts on Windows XP](http://technet.microsoft.com/en-us/library/bb456992.aspx).
* [Best Practices for Delegating Active Directory Administration](http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3&DisplayLang=en).
* [*IT Compliance Management Guide*](http://go.microsoft.com/fwlink/?LinkId=56419).
* [MSDN Industry Center - Banking - Downloads](http://msdn2.microsoft.com/en-us/architecture/86e3451d-8219-46af-bf99-4a610e4bf1f4.aspx).
* [Navigating PCI DSS – Understanding the Intent of the Requirements](https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_navigating_dss.pdf) (PDF).
* PCI DSS version 1.2 (PDF)
* [PCI SSC New Self-Assessment Questionnaire](https://www.pcisecuritystandards.org/saq/index.shtml).
* [Payment Card Industry (PCI) Data Security Standard Security Audit Procedures](https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf) (PDF).
* [Payment Card Industry (PCI) Data Security Standard Security Scanning Procedures](https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf) (PDF).

## Feedback

Please direct questions and comments about this guide to the [Compliance Management Forum](http://social.technet.microsoft.com/Forums/en-US/compliancemanagement/threads/). The forum provides the opportunity to join discussions and collaborate on GRC–related compliance management issues with your peers.

# Acknowledgments

The Solution Accelerators – Security and Compliance (SA-SC) team would like to acknowledge and thank the team that produced the *Payment Card Industry Data Security Standard (PCI DSS)* *Compliance Planning Guide*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this guidance.

**Authors**

Frank Simorjay

TwC Computing group

**Program Manager**

Frank Simorjay

**Editors**

John Cobb - *Wadeware LLC*

Steve Wacker - *Wadeware LLC*

**Test Manager**

Sumit Parikh

**Testers**

Praveen Palakkazhi - *Infosys Technologies Ltd*

Amit Sadana - *Infosys Technologies Ltd*

**Release Manager**

Karina Larson

## Contributors and Reviewers

Jeff Elliot – *QSA - Protiviti*, Jason Harper – *Protiviti*, Andrew Law, Bruce Lobree – *Senior Risk Management Analyst - Nintendo of America Inc.*, Brandon Lowther – *QSA - Protiviti*, Jeffrey Miller, Sai Sireesh Pachava, Jed Pickel, Jeff Sanchez – *National PCI Practice Lead and QSA - Protiviti*, Daniel Taylor, Pat Telford