
May 2007
Microsoft Health and Life Sciences
Microsoft Consulting Services
Table of Contents

Introduction .................................................................................................................. 3
Table 1: Map of Microsoft Technology Relevant Technologies to 21 CFR Part 11
Requirements ............................................................................................................. 6
Subpart B Electronic Records ....................................................................................... 7
11.10 Controls for Closed Systems ............................................................................ 7
  11.10 (a) Validation of Systems ............................................................................. 7
  11.10 (b) Record Review and Inspection .............................................................. 10
  11.10 (c) Records protection and retrieval ......................................................... 11
  11.10 (d) System Access .................................................................................... 14
  11.10 (e) Audit Trail .......................................................................................... 15
  11.10 (f) Operational System Checks ................................................................. 20
  11.10 (g) Protect records from unauthorized access .......................................... 22
  11.10 (h) Data Input Validation .......................................................................... 23
  11.10 (i) Training .............................................................................................. 24
  11.10 (j) Electronic Signature Policy ................................................................. 24
  11.10 (k) System control .................................................................................. 25
  11.30 Controls for Open Systems ......................................................................... 29
  11.50 Signature Manifestations .......................................................................... 31
    11.50 (a) Signature Manifestation .................................................................. 31
    11.50 (b) Control of signature information .................................................... 33
  11.70 Signature/Record Linking .......................................................................... 33
Subpart C Electronic Signatures .............................................................................. 34
  11.100 General Requirements ........................................................................... 34
    11.100 (a) Uniqueness .................................................................................. 34
    11.100 (b) Identity Verification ...................................................................... 34
    11.100 (c) Legal Certification ........................................................................ 34
  11.200 Electronic Signature Components and Controls ..................................... 35
    11.200 (a) Non-biometric Signatures ............................................................. 35
    11.200 (b) Biometric Signatures .................................................................. 39
  11.300 Controls for Identification Codes/Passwords .......................................... 39
    11.300 (a) Uniqueness of identity .................................................................. 39
    11.300 (b) Password Policy .......................................................................... 40
    11.300 (c) Deactivation of Users .................................................................. 40
    11.300 (d) Unauthorized use of passwords or identification codes ............... 41
    11.300 (e) Identification Code Device Testing .............................................. 41
Systems Validation and Compliance ........................................................................ 42
References ............................................................................................................... 43
Introduction

Compliance is a major focus area for Microsoft and the Office 2007 system. During design and development, specific attention was paid to features that enable regulated document management, including:

- Audit trails
- Record and document retention policies
- Document level security
- Open file formats (OpenXML and XPS) that allow documents to be machine readable, human readable, and consistent in presentation across systems
- A consistent, thorough secure software development methodology (Security Development Lifecycle) that was applied to all the applications mentioned herein

While these features can be applied to a broad range of regulations, including Sarbanes-Oxley and HIPAA, they also apply to 21 CFR Part 11. Thus, the Microsoft Office SharePoint Server 2007 (MOSS 2007), when combined with other Microsoft technologies, including Active Directory, Information Rights Management, and (optionally) the Microsoft PKI system, provides a system that may be configured to assist with 21 CFR Part 11 compliance when implemented as part of a broader compliance framework. Although most software cannot be compliant by itself, the use of MOSS 2007 and other Microsoft technologies can be implemented as a component of a broader framework of policies, procedures, and other systems that are put in place by the implementing party.

The following pages provide a table mapping of 21 CFR Part 11 sections to the Microsoft relevant technologies that can assist with compliance. This white paper will not only describe the regulation, but will also detail the specific features and configurations of SharePoint, Office 2007, Internet Information Server (IIS), Windows Server, Windows Rights Management Service, ASP.NET, and Active Directory, including actions to take along with example screenshots.

This white paper may also be helpful for validation purposes, including but not limited to: providing guidance in developing test plans, pointing out areas to test for proper configuration of the system, documentation of the steps taken when in an audit situation, and detailing the development methodology used in producing the Office 2007 system.
<table>
<thead>
<tr>
<th>Subpart B</th>
<th>Relevant Microsoft Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.10 Controls for closed systems</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (a) Validation of systems</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (b) Record review and inspection</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (c) Records protection and retrieval</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (d) System access</td>
<td>Windows (IIS, Active Directory, ASP.NET)</td>
</tr>
<tr>
<td>11.10 (e) Audit trail</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (f) Operational system checks</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (g) Protect record from unauthorized access</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (h) Data input validation</td>
<td>Windows, ASP.NET, Forefront</td>
</tr>
<tr>
<td>11.10 (i) Personnel training</td>
<td>Not applicable</td>
</tr>
<tr>
<td>11.10 (j) Electronic signature policy</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.10 (k) System control</td>
<td>Windows (Rights Management) and Office 2007 Systems</td>
</tr>
<tr>
<td>11.30 Controls for open system</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.50 Signature manifestation</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.50 (a) Signature information</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.50 (b) Control of signature information</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>11.70 Signature/record linking.</td>
<td>Office 2007 Systems</td>
</tr>
<tr>
<td>Subpart C</td>
<td>Electronic Signatures</td>
</tr>
<tr>
<td>11.100 General requirements.</td>
<td>Not applicable</td>
</tr>
<tr>
<td>11.100 (a) Uniqueness</td>
<td>Not applicable</td>
</tr>
<tr>
<td>11.100 (b) Identity verification</td>
<td>Not applicable</td>
</tr>
<tr>
<td>11.100 (c) Legal certification</td>
<td>Not applicable</td>
</tr>
<tr>
<td>11.200 Electronic signature components and controls</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.200 (a) Non-biometric signature</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.200 (b) Genuine use of biometrics signature</td>
<td>Windows and Office 2007 Systems</td>
</tr>
<tr>
<td>11.300 Controls for credentials</td>
<td>Windows (Active Directory)</td>
</tr>
<tr>
<td>11.300 (a) Maintain of credentials uniqueness</td>
<td>Windows (Active Directory)</td>
</tr>
<tr>
<td>11.300 (b) Credential maintenance</td>
<td>Windows (Active Directory)</td>
</tr>
<tr>
<td>11.300 (c) Process for lost or compromised credentials</td>
<td>Windows (Active Directory)</td>
</tr>
</tbody>
</table>
Subpart B Electronic Records

11.10 Controls for Closed Systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

The following is a discussion of how the Microsoft Office system may address these requirements, with the specific procedures and controls further detailed in the subsections following this section.

SharePoint Server addresses authenticity, integrity and confidentiality of electronic records through access control and permission to the records on either the individual record level or a document library level. Users are assigned permissions to content and records through permissions which limit what they can do by administrators. Documents identified as records can be sent to a record center for safe keeping and have separate access control than when the document was authored and reviewed.

To protect confidentiality of an electronic record, documents can be protected by Information Rights Management (IRM) policy that could restrict users from copying or printing documents even after the document is saved outside of the SharePoint Server.

SharePoint also addresses non-repudiation through audit trails. SharePoint provides an auditable system of records - audit policies can be configured for documents and items in Office SharePoint Server 2007 to specify which events will be audited for each Content Type or site level, via the Information Management Policy capabilities. An audit trail is kept with a document throughout the document and record life cycle.

11.10 (a) Validation of Systems

Systems validation ensures accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

How Office 2007 System addresses the requirement

Addressing this requirement takes a couple forms: 1) Validation of the system as a whole, and 2) validation of the individual documents or records.
To address validation of the system, there are three areas of validation that implementing parties need to be concerned with: IQ (Installation Qualification), OQ (Operational Qualification) and PQ (Performance Qualification).

In the case of Installation Qualification, the focus is on ensuring that the application is installed correctly, and all Microsoft product generated installation logs are maintained which detail the installation as well as any errors that may arise during the installation process.

Operational Qualification begins with the development methodology utilized to create the software. Most Microsoft products, and all the products detailed in this whitepaper, adhere to the "Security Development Lifecycle" methodology. This methodology, which encompasses steps traditionally employed in software development methodology, places a particular focus on development of software that is secured by design, in development, and through implementation. All major software releases from Microsoft, beginning with the Office 2007 and Vista/Longhorn "wave" of software releases are required to go through the internal processes and checkpoints detailed in the Security Development Lifecycle methodology, and must be signed off on by a Security Officer before the particular software can be released to the general public.

The details of the methodology are available on MSDN as well as through published works by Steve Lipner and Michael Howard (see the Reference section for more information).

Operational Qualification extends to the operation of the software. To that end, most Microsoft software, and all the products detailed in this whitepaper, provide detailed error logging and troubleshooting information that can be gained through a proper implementation of the Microsoft Operations Manager (or MOM). In fact, any software release must include a management pack for MOM before the particular software can be released to the general public.

The details of the MOM management pack for all relevant software are available in the References section of this document.

Performance Qualification always includes the question -- "Does the software perform to the end users' needs?" As that question can only be answered by the implementing party, the final step in validation of the software needs to be the development of test plans and testing of the software in the environment in which it will be utilized. These test plans can be modeled on this whitepaper to assist with the proper configuration of the software.

While the overall validation of the software is up to the implementing party, Microsoft has assisted in the validation through the creation of the development methodology, implementation of the MOM management packs, implementation of the installation logs, and development of this whitepaper to give guidance in the configuration of the software and development of the test plans for performance qualification.
Finally, Microsoft recommends that companies periodically audit their own implementation of the software, in order to ensure that the guidelines specified herein are applied to their production systems and are enforced throughout.

To address validation of the individual documents, SharePoint provides auditing features to facilitate the validation process.

As SharePoint server is designed as an auditable system, the administrator can configure the system to audit document creation, specifically document modification and deletion among other things so all changes to a document are audited. Additionally, you can also extend the auditing capabilities to include additional information such as version and workflow status.

For Document level, you have the following out-of-box choices of auditable events. This can be configured on site collection level, document and list, or content-type level.

<table>
<thead>
<tr>
<th>Auditing</th>
<th>Enable Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the events that should be audited for documents and items subject to this policy.</td>
<td>Specify the events to audit:</td>
</tr>
<tr>
<td>- Opening or downloading documents, viewing items in lists, or viewing item properties</td>
<td>- Editing items</td>
</tr>
<tr>
<td>- Checking out or checking in items</td>
<td>- Moving or copying items to another location in the site</td>
</tr>
<tr>
<td>- Deleting or restoring items</td>
<td></td>
</tr>
</tbody>
</table>

To configure a document library, select Document Library Settings (as shown below) from the document library’s settings menu and then select “Information management policy settings” under the Permissions and Policies section.

For content type, you can define this under content type’s Settings and then “Information management policy settings”.

For site collection level, the configuration is the same as configuring site level auditing events discussed below.
SharePoint Server also enables the audit of site level for the following events as shown below. To set this setting, follow the flow below to the Top Level Site Settings if you are not currently on the top level site:

Site Actions -> Site Settings -> Top to Top Level Site Settings

Under Site Collection Administration, select “Site collection audit settings”.

11.10 (b) Record Review and Inspection

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

How Office 2007 System addresses the requirement

Documents stored in SharePoint in their native format can be viewed with their corresponding viewer application.

Additionally, Microsoft Office SharePoint Server 2007 includes an extensible framework and runtime support to enable your own custom document converters for the document libraries in a Web application. A document converter is a custom executable file that
takes a document of one file type, and generates a copy of that file in another file type.
Using document converters, you can transform your content into different versions to suit
your business needs. Converter will respect IRM rights associated with the document.

For examples of document converter implementation, please refer to the ECM start kit at:

Additionally, when the documents in question are written in the Microsoft Office 2007
system, the new OpenXML file format allows the document to be accessible
electronically (i.e. machine readable in XML in its component parts) while still
maintaining the ability to be viewed as a whole through Word, Excel, or PowerPoint as
appropriate. Saving the document in XML Paper Specification (XPS) format provides the
best of both worlds: a machine readable document (in XML) whose formatting does not
change regardless of the printer, screen, or viewing application used to display the
document.

A description of the OpenXML format is found at: http://www.ecma-
international.org/publications/standards/Ecma-376.htm

A description of the XML Paper Specification (XPS) is found at:
http://www.microsoft.com/whdc/xps/downloads.mspx

Both XPS and OpenXML are native file formats for Office 2007 and are understood and
readable by the Vista operating system as well.

Agencies and inspectors can be given read-only access to documents during the review
process. Electronic documents will be viewed either natively or in other formats via
document converters or viewers.

11.10 (c) Records protection and retrieval
Protection of records to enable their accurate and ready retrieval throughout the records
retention period.

How Office 2007 System addresses the requirement
Microsoft Office SharePoint Server 2007 Records Centers can be organized to match
your file plan. The policies for content in the site can be configured to match your
retention schedules, and the metadata for that content can be set up to capture whatever
information you need for the long-term management of those records. Record managers
can use the record center to:

1) Automatically receive/route records declared from other sources—Records
Centers are able to determine how the Content Type of a declared record
translates to an appropriate record series in the file plan, and then file the record
into the appropriate location.
2) Hold orders—The Records Center includes a powerful hold order system to locate records relevant to particular event requiring a hold order, suspending disposition of those records for the duration of the event, and for resuming normal disposition once those events have ended.

3) Separate access controls—Records Center can give you the flexibility to specify whether users can access any section of the Records Center, whether they can view or add items, independent of the permissions those users have on authoring and collaboration sites.

Documents can be attached to a policy that defines content expiration and version control policy.

Information Management Policy allows records managers and administrators to specify a “policy” that defines how the system should handle content so that it is compliant with a records management program and given regulations. Policies can be defined and attached to content types, document libraries & lists in collaborative and records spaces so that once the policies are applied, all content classified within that content type or location will automatically be managed in accordance with that policy, without any active end-user participation.

The following is a screenshot of a policy definition page for a content type:
Microsoft Office technology allows content that is outside the repository to be secured on the basis of policies as well by using the Rights Management Server. With the 2007 system, an access control policy set up for a SharePoint site can also be maintained for
documents on the desktop. These rights also extend to expiration, printing, forwarding, and copying, thereby ensuring a higher level of content security than has been possible with traditional approaches.

11.10 (d) System Access
Limiting system access to authorized individuals

How Office 2007 System addresses the requirement
SharePoint sites containing information or documents to be protected should not allow anonymous access. The User will need to be authenticated before access to the site is granted.

The following are authentication methods for SharePoint (or any ASP.NET application):
- Windows integrated (NTLM, Kerberos, or certificate) – user is authenticated when they log on their computer. This is enforced by IIS.
- Basic authentication – user enters domain credentials for authentication before access to the site is granted. This is enforced by IIS. As credentials are sent as plain text by default, this option should use SSL or other mechanism to encrypt the http traffic.
- Forms based or SSO – user enters credentials assigned to them that may not be their domain credentials. As with Basic Authentication, HTTP traffic needs to be encrypted to protect the credentials. This requires additional settings on web.config file for the web application.

Authentication setting is set per web application (the container that hosts portal and collaboration sites) and is configured through SharePoint Central Administration Application.

The following is a sample web.config file used to setup forms-based authentication, role-based access, and denies access to unauthenticated users:

```xml
<configuration>
  <connectionStrings>
    <add name="MySqlConnection" connectionString="Data Source=MySqlServer;Initial Catalog=aspnetdb;Integrated Security=SSPI;" />
  </connectionStrings>
  <system.web>
    <authentication mode="Forms">
      <forms loginUrl="login.aspx" name=".ASPXFORMSAUTH" />
    </authentication>
    <authorization>
      <deny users="?">
      </deny>
    </authorization>
  </system.web>
</configuration>
```
After authentication, the user will also need to be assigned appropriate rights to access specific features and contents. Details on how to configure user roles and rights are discussed in Section 11.10 (g) of this paper.

11.10 (e) Audit Trail

Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
How Office 2007 System addresses the requirement

As discussed in 11.10 (a) audit trails in SharePoint are provided at the document level, are sequential by machine date, and capture associated meta-data with the document including operator, document location, and action taken on the document. These audit trails are kept in association with the document throughout its life cycle.

Out of box, you can access the audit log at site collection level from the Site Actions menu and then select “Audit log reports” from Site Collection Administration section.

View Auditing Reports

Use these reports to view Audit Log data collected for this Site Collection.

- **Content Activity Reports**
  - **Content modifications**
    - This report shows all events that modified content in this site.
  - **Content type and list modifications**
    - This report shows all events that modified content types and lists in this site.
  - **Content viewing**
    - This report shows all events where a user viewed content in this site.
  - **Deletion**
    - This report shows all events that caused content in this site to be deleted or restored from the Recycle Bin.

- **Custom Reports**
  - **Run a custom report**
    - Manually specify the filters for your Audit Report.

- **Information Management Policy Reports**
  - **Expiration and Disposition**
    - This report shows all events related to the expiration and disposition of content in this site.
  - **Policy modifications**
    - This report shows all events related to the creation and use of information management policies on content in this site.

- **Security And Site Settings Reports**
  - **Auditing settings**
    - This report shows all events that change the auditing settings of Windows SharePoint Services.
  - **Security settings**
    - This report shows all events that change the security configuration of Windows SharePoint Services.

An example of running a custom report:
It is possible to view the audit history as a site feature with a couple lines of ASP code. The following code snippet will provide a site-wide audit trail function which facilitates viewing the audit history by reviewing parties.

To implement a customized audit trail report view, you create a regular ASPX page that inherits from an existing SharePoint master page. Below is an example of ASPX page attributes:

```csharp
%@ Page Language="C#" Src="MyAudit.aspx.cs" AutoEventWireup="true"
Inherits="MyNameSpace.MyAudit" MasterPageFile="~/_layouts/application.master"
```

Following is an example of a customized audit trail report feature:
The resulting audit history view:
Audit History: Contract Management

The table below lists the audit history for this item.

<table>
<thead>
<tr>
<th>Date</th>
<th>User</th>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/5/2006 6:38:19 PM</td>
<td>Mike Ray</td>
<td>Update</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:38:20 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:38:20 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:38:21 PM</td>
<td>Mike Ray</td>
<td>CheckOut</td>
<td>v0.1</td>
</tr>
<tr>
<td>6/5/2006 6:38:46 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:38:47 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:38:47 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:38:48 PM</td>
<td>Mike Ray</td>
<td>CheckIn</td>
<td>v0.1</td>
</tr>
<tr>
<td>6/5/2006 6:39:17 PM</td>
<td>Mike Ray</td>
<td>CheckOut</td>
<td>v0.1</td>
</tr>
<tr>
<td>6/5/2006 6:39:19 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:39:20 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:39:29 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:40:29 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:40:29 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:40:30 PM</td>
<td>Mike Ray</td>
<td>CheckIn</td>
<td>v0.2</td>
</tr>
<tr>
<td>6/5/2006 6:40:31 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:40:43 PM</td>
<td>Mike Ray</td>
<td>CheckOut</td>
<td>v0.2</td>
</tr>
<tr>
<td>6/5/2006 6:41:11 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:41:11 PM</td>
<td>Mike Ray</td>
<td>Update</td>
<td>v0.3</td>
</tr>
<tr>
<td>6/5/2006 6:41:12 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:41:12 PM</td>
<td>Mike Ray</td>
<td>View</td>
<td></td>
</tr>
<tr>
<td>6/5/2006 6:41:13 PM</td>
<td>Mike Ray</td>
<td>CheckIn</td>
<td>v0.3</td>
</tr>
</tbody>
</table>

An audit trail can be extended relatively easily to record any additional information as shown below in a code snippet from an event handler that writes a custom event to the audit trail associated with the list item which can be a document:

```csharp
SPLListItem checkedinItem = eventProperties.ListItem;
checkedinItem.Audit.WriteAuditEvent(SPAuditEventType.Custom, "Event source such as signature", "Additional information you may have…");
```

While users of collaborative spaces can be given full rights to active content, the audit log is tightly restricted. Only administrators (or users who are granted sufficient privileges) are able to view the audit history, using Microsoft Office Excel-based reports. And no user can selectively edit or delete individual audit entries. There are some built in reports including Deleted event reports (accessed through the “Site Actions” drop down menu. Select “Site Settings”, and then select “Audit log reports” under the Site Collection Administration column of the site settings page). See below.
The Deletion report shows details of the events:

<table>
<thead>
<tr>
<th>Site Id</th>
<th>Item Id</th>
<th>User Id</th>
<th>Document Location</th>
<th>Occurred (GMT)</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>77752d52-594-4ae3fda9211c453e-4f9c7f81f4e52a2</td>
<td>1</td>
<td>1</td>
<td>\file{\siteurl}/Shared Documents/test.pdf</td>
<td>2007-01-15T01:06:01</td>
<td>Delete</td>
</tr>
</tbody>
</table>

**11.10 (f) Operational System Checks**

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate

**How Office 2007 System addresses the requirement**

SharePoint 2007 can enforce check in/out policy on document libraries. Under checkout policy, a user can only view documents without checkout and has to checkout the document before editing.

Check out policy is set via Versioning Settings off of the document library’s General Settings section as shown below:
For libraries with “Require Check Out” checked, the user will open a document as ‘read only’ when clicking on the document link by default and will need to check the document out before editing as shown below:

SharePoint 2007 workflow capability enables automated business processes, such as document review and approval processes, based on the sequence of events prescribed in the organizational policies. The sequence of events associated with a particular workflow is tracked and enforced.
11.10 (g) Protect records from unauthorized access

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

How Office 2007 System addresses the requirement

SharePoint Server 2007 (via WSS v3) controls access to Web sites, lists, folders, and list items through a role-based membership system by which users are assigned to roles that authorize their access to Windows SharePoint Services objects. The creation and authentication of the user and to which role the user is assigned is discussed in Section 11.300 – Controls for Identification Codes / Passwords.

To give a user access to an object, you either add the user to a group that already has permissions on the object, or create a role assignment object, setting the user for the role assignment and then adding the assignment to the collection of role assignments for the object (such as list item, folder, list, or Web site).

Windows SharePoint Services includes the following three groups by default:

- owners (administrator)
- members (contributor)
- visitors (reader)

You can either add new groups or customize existing groups to fine tune permission sets for users. You can access the People and Group screen by selecting the Site Actions -> Site Settings page under the Users and Permissions section to define new groups and adding users to groups:

By default, objects inherit permissions from their parent (document from document library or folder, document library from site, site from parent site).

Following are the screen shots of defining a unique permission setting for a document. The process is the same for library and site.
Confirmation dialog for defining unique permissions different from parent:

![Confirmation dialog for defining unique permissions different from parent](image)

An example of fine tuning a particular group’s rights:

![An example of fine tuning a particular group’s rights](image)

11.10 (h) Data Input Validation

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

How Office 2007 System addresses the requirement

Transport level encryption (such as SSL) can be used to secure the content (data input) from users.

ASP.NET (which SharePoint is built on) uses the Message Authentication Code (MAC) technique to protect key information, such as view state data and authentication tickets, to make sure that the data are not illegally modified.

For cookie-based authentication (such as forms authentication), administrators can configure cookie timeout parameters to be reasonably short to reduce the cookie reply security risk.
For additional protection, Microsoft has developed Forefront Security for SharePoint, which helps businesses protect their Microsoft Office SharePoint Portal Server 2007 and Windows SharePoint Services 3.0 servers from viruses, unwanted files and inappropriate content. With a layered, multiple scan engine approach, Forefront Security for SharePoint helps stop the latest threats before they impact your business and users.

11.10 (i) Training
Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

How Office 2007 System addresses the requirement
Microsoft product teams follow rigorous development and testing processes for its product development including the Office 2007 systems, as described in Section 11.10(a) Validation of Systems.

Microsoft and many of its partners offer extensive training courses, technical resources, and certifications for .NET, SharePoint and related technologies to help organizations to educate and train their people for specific tasks.

11.10 (j) Electronic Signature Policy
The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

How Office 2007 System addresses the requirement
Creating a successful Records Management system starts with mapping out the organization’s records management goals, anticipating the challenges an organization will face in making that vision a reality within the company, and developing a policy and implementation that fits these needs. Since planning is a key to both the policy development and solution implementation phases, it is important to outline the challenges faced at each stage so these can be kept top of mind when working out both the organization policy plan and implementation strategy.

At the policy planning stage, the major challenge is to devise a system that encompasses an organization’s current records-keeping needs: content types, media types, storage requirements, business processes, and policies. It also needs to meet present legal and audit requirements, and be extensible and flexible enough to accommodate future content types and retention requirements. Another important goal is to enhance information retrieval, which will help employees do their jobs more efficiently and give an organization a competitive advantage.
In developing the policy for an organization, the challenge is to create an overarching policy document that is comprehensive but short, easy to read, and accompanied by actionable retention schedules that can then be put into practical use. Furthermore the policy needs to be integrated with the organization’s other enterprise content management policies, and be able to absorb and integrate previous record keeping efforts.

At the implementation stage, the major challenge is to create a system that suits the organization’s workflow, one that will actually be adopted by users and integrated into their daily activities. The implementation must be simple enough for employees to grasp quickly, easy enough to require only few extra steps (or clicks), but rigorous enough to meet the organization’s overall need for record keeping within the organization. Furthermore, any technology rollout must be manageable for the organization as a whole – and not significantly disrupt normal business operations.

Microsoft Office SharePoint Server 2007 includes four information management policy features to help an organization manage content type as shown in Section 11.10 (c):

- Document expiration
- Document auditing
- Document labels
- Document bar codes

11.10 (k) System control
Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

How Office 2007 System and Rights Management Services (RMS) address the requirement
Microsoft Windows Rights Management Services (RMS) augments an organization’s security strategy by providing protection of information through persistent usage policies, which remain with the information. Content is protected with RSA 1024-bit Internet encryption and authentication so that information will be safe in transit and will remain with the document, no matter where it goes. For example, encrypted content stored on a lost USB drive will not be accessible and viewable to any unauthorized viewer, regardless of location.

This information protection technology works with RMS–enabled applications to help safeguard digital information from unauthorized use—both online and offline, inside and outside of the firewall. Record managers and administrators can define exactly how users can use data and can place limitations on who can open, modify, print, copy, and forward certain confidential information.
Document permission can be restricted through Office 2007. The following is the screenshot from Word 2007 showing access to the “Restrict Permission” menu:

To set specific permission and restriction, select from the following:
For example, a document opened by a user who has read-only access will not be able to print and copy the document as seen below:
RMS (SP2) enables Information Rights Management (IRM) in Microsoft Office SharePoint Server 2007. IRM for SharePoint 2007 can be enabled through the central administration page:

Revision and change control can be enforced through checkout and audit trail policies as discussed previously in this document.
11.30 Controls for Open Systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Section 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

How Office 2007 System addresses the requirement

SharePoint can leverage the underlying ASP.NET infrastructure to authenticate users through various means which are discussed in Section 11.300 – Controls for Identification Codes / Passwords. Together with SSL (or other transport level security measures), user access and data transport can be secured from the point of creation to the point of receipt.

Office 2007 enables three use-case scenarios with the out-of-the-box digital signature functionality to protect documents starting from their point of creation.

- Authenticity & Tamper Resistance – Signing an Office document to prove that it hasn’t been modified since it was signed. You can also view the digital certificate used to sign the document to verify the authenticity of the document and prove that it came from a trusted individual or organization.

- Digital Signature – Signing an Office document with both a specific identity and an assertion about why this document was signed (for example, “Approved for Publication”). This type of signature does not print with a document and does not affect the on-page content of a document, but can be viewed and verified with software, including Office 2007 applications.

- In Document Signature – Signing an Office document in a special “signature line” object that visually shows who signed the document. This feature is designed to mimic the experience of pen and ink signatures.

Office 2007 documents support digital signatures out of the box and are extensible. For digital signature of non-office based documents, there is 3rd party vendor support in the market place.

This screenshot below shows how a Word document is signed with required information:
See below for a document with signature capture and a signature task pane:
In addition to the digital signature controls and SSL used to transmit the electronic record, Forefront Security for SharePoint can provide further assurance that the record is valid by protecting Microsoft Office SharePoint Portal Server 2007 and Windows SharePoint Services 3.0 servers from viruses, unwanted files and inappropriate content.

11.50 Signature Manifestations

11.50 (a) Signature Manifestation
Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
(1) The printed name of the signer;
(2) The date and time when the signature was executed; and
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

How Office 2007 System addresses the requirement
SharePoint 2007 can use workflow to enforce document approval and signoff. Information collected during the approval and signoff process can be customized to include all information required under this rule and more. Custom solutions built on top of the Office SharePoint Server 2007 can also add relevant entries to the audit log, such as when an approval workflow is completed.

You can access workflow information through "Workflow” link off of document’s context menu:
The below figure shows a list of workflows this sample document has gone through:

<table>
<thead>
<tr>
<th>Workflows</th>
<th>Name</th>
<th>Started</th>
<th>Ended</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running Workflows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completed Workflows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Below shows the detailed information for the selected sample workflow:
11.50 (b) Control of signature information

The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

How Office 2007 System addresses the requirement

Office 2007 documents store digital signatures as a separate stream from the content stream and are part of the document package. As shown in previous screen shots, the digital signature of an Office 2007 document can mimic the paper and ink signature experience.

In the case of Electronic Signatures, the signature, date and time of signature, and the signature meaning are linked to the document through metadata that is associated with the document in SharePoint; are kept with and linked to the document throughout the document life cycle; and can be viewed with the document in SharePoint. It is possible to integrate the metadata into the body of the document, as it would appear in a printed version of the document, through the use of a document template that reads the metadata from SharePoint, stores the metadata in the document as part of the OpenXML, and then allows for display of the metadata inline in the document.

11.70 Signature/Record Linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

How Office 2007 System addresses the requirement

Digital signatures for Office 2007 documents are stored as part of the document. Office 2007 provides a task pane to help users view and verify the signatures stored within a
document. This pane is designed to differentiate signatures based on whether they are requested, valid, or invalid. This task pane is a built-in part of the signature platform and automatically displays information about the signature objects regardless of whether they come from our built-in implementation or a custom written signature add-on. Please refer to Section 11.30 for screenshots of a document with a digital signature and task pane.

Electronic signature and approval information are stored as part of the audit trail and metadata associated with the document. The linkage between signature and document is maintained by the server and can be read in the document through document templates as discussed in the previous section.

Subpart C Electronic Signatures

11.100 General Requirements

11.100 (a) Uniqueness
Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

How Office 2007 System addresses the requirement
Policies and procedures should be developed to verify each user’s identity prior to a user being assigned a username and password and to dictate that users should not share credentials. These policies and procedures should be included as part of the compliance and system training process.

The creation, maintenance, and authentication of the user are discussed in Section 11.300 – Controls for Identification Codes / Passwords.

11.100 (b) Identity Verification
Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

How Office 2007 System addresses the requirement
This should be part of the compliance solution planning and training process.

11.100 (c) Legal Certification
Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.
The certification shall be submitted in paper form and signed with a traditional
handwritten signature, to the Office of Regional Operations (HFC 100), 5600 Fishers
Lane, Rockville, MD 20857.

Persons using electronic signatures shall, upon agency request, provide additional
certification or testimony that a specific electronic signature is the legally binding
equivalent of the signer's handwritten signature.

**How Office 2007 System addresses the requirement**

In addition to this being part of the compliance solution planning process, a step can be
added to the signing workflow to verify that a certification check is in place (by looking
at a lookup list of authorized signers).

**11.200 Electronic Signature Components and Controls**

**11.200 (a) Non-biometric Signatures**

Electronic signatures that are not based upon biometrics shall:

1. Employ at least two distinct identification components such as an identification code
   and password.
   1. (i) When an individual executes a series of signings during a single, continuous period
      of controlled system access, the first signing shall be executed using all electronic
      signature components; subsequent signings shall be executed using at least one electronic
      signature component that is only executable by, and designed to be used only by, the
      individual.
   1. (ii) When an individual executes one or more signings not performed during a single,
          continuous period of controlled system access, each signing shall be executed using all of
          the electronic signature components.
2. Be used only by their genuine owners; and
3. Be administered and executed to ensure that attempted use of an individual's
   electronic signature by anyone other than its genuine owner requires collaboration of two
   or more individuals.

**How Office 2007 System addresses the requirement**

SharePoint supports variety of authentication mechanisms supporting 2 factor schemes
(combination of user id and password). This includes windows integrated (NTLM and
Kerberos) authentication and basic authentication and forms authentication. Whether an
organization only requires the user to enter one component or both during a signing
session is part of the workflow design process. Workflow can track previous signing
timestamps and a session token can be used to decide if the user is part of the continuous
period of access to determine if it is required to:

- Only ask for one component if it determines a continuous session or
- Request for both signature components if it is not a continuous session

Users should not share their credentials. A user has to be authenticated before gaining
access to the application and a user can only sign on as him or herself.
The site administrator can reassign tasks such as approval and signature from one person to another. Regardless, the reassigned person has to authenticate first to carry out the task. These actions can be further captured by the audit trail.

The following is an example of implementing a simple electronic signature for a document library for any type of document:

1) Enable auditing for the library. Auditing can also be enabled on site level.
2) Add necessary document metadata to keep track of document and signature status and who should sign the document.

The following screen shot shows that a word and a PDF file are waiting to be signed.

Shared Documents

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Created By</th>
<th>Modified By</th>
<th>Signed</th>
<th>WorkflowStatus</th>
<th>Signer</th>
<th>CollectSignature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2007-01-09T12_09_59</td>
<td>System Account</td>
<td>Brian Cox</td>
<td>No</td>
<td>Pending</td>
<td><a href="mailto:luis@libwarsinc.com">luis@libwarsinc.com</a></td>
<td>In Progress</td>
</tr>
<tr>
<td></td>
<td>test doc</td>
<td>System Account</td>
<td>Brian Cox</td>
<td>No</td>
<td>Approved</td>
<td><a href="mailto:luis@libwarsinc.com">luis@libwarsinc.com</a></td>
<td>In Progress</td>
</tr>
<tr>
<td></td>
<td>test pdf document</td>
<td>new</td>
<td>Brian Cox</td>
<td>Brian Cox</td>
<td>No</td>
<td>Approved</td>
<td><a href="mailto:luis@libwarsinc.com">luis@libwarsinc.com</a></td>
</tr>
</tbody>
</table>

3) Create a workflow to collect user signature based on the status from specified signer.

The following workflow is created through SharePoint Designer without needing to write any custom code.
Here are the tasks assigned to LuisB as result of the workflow:

**Tasks**

<table>
<thead>
<tr>
<th>Title</th>
<th>Assigned To</th>
<th>Status</th>
<th>Priority</th>
<th>Due Date</th>
<th>% Complete</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your signature is required for this document</td>
<td>Luis Bonfaz</td>
<td>Not Started</td>
<td>Normal</td>
<td></td>
<td></td>
<td>test doc</td>
</tr>
<tr>
<td>Your signature is required for this document</td>
<td>Luis Bonfaz</td>
<td>Not Started</td>
<td>Normal</td>
<td></td>
<td></td>
<td>test pdf</td>
</tr>
</tbody>
</table>

In order for LuisB to complete these tasks, the following must be done:

1) Click on the Edit Item context menu to complete the task:
2) Enter needed information to complete the task:

<table>
<thead>
<tr>
<th>Title:</th>
<th>Your signature is required for this document</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID:</td>
<td>Luisb</td>
</tr>
<tr>
<td>Pin:</td>
<td>12345</td>
</tr>
<tr>
<td>Comments:</td>
<td>I sign this document</td>
</tr>
<tr>
<td>Related list item:</td>
<td>test pdf document</td>
</tr>
</tbody>
</table>

4) Create a custom audit trail to record the signature signed to the document (optionally checksum when the document is signed). Below is a sample code snippet (in C#) that writes signature name to the audit trail:

```csharp
public override void ItemUpdated(SPItemEventProperties properties)
{
    SPListItem savedItem = properties.ListItem;
    string status = savedItem.Properties["WorkflowStatus"].ToString();
    string signed = savedItem.Properties["Signed"].ToString();
    if (bool.Parse(signed))
    {
    }
```
string signer = savedItem.Properties["Signer"].ToString();

savedItem.Audit.WriteAuditEvent(SPAuditEventType.Custom, "Signature", "<signature> Signed by: " + signer + "</signature>");

A custom event handler captures the signature information to the audit trail as shown below (viewed through custom audit report):

<table>
<thead>
<tr>
<th>Item Type</th>
<th>User Id</th>
<th>Document Name (GMT)</th>
<th>Event</th>
<th>Source Name</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document</td>
<td>LITWAREINC\brian</td>
<td>ib/ITSiteCo_2007-01-15T03:29:05</td>
<td>Custom Signature</td>
<td>&lt;signature&gt; Signed by: <a href="mailto:luisb@litwareinc.com">luisb@litwareinc.com</a>&lt;/signature&gt;</td>
<td></td>
</tr>
</tbody>
</table>

11.200 (b) Biometric Signatures
Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

How Microsoft Windows and Office 2007 addresses the requirement
There are 3rd party vendors who provide biometric-based authentication to the Windows system, including most major hardware vendors. With respect to the Microsoft Office 2007 system, a biometric identity is handled as any other identity, as the biometric information is associated with either a username or a digital certificate. Regardless, a password is still required for authentication (in the case of electronic signatures), or a PIN is required for authentication (in the case of a Digital Certificate).

11.300 Controls for Identification Codes/Passwords
Persons who use electronic signatures based upon the use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include the following:

11.300 (a) Uniqueness of identity
Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

How Microsoft Windows and Active Directory addresses the requirement
This is enforced by Windows or Active Directory if using integrated authentication and Basic authentication in an organization’s SharePoint setup.
For detailed discussion as well as a step-by-step configuration guide of windows accounts and password policy, please refer to the articles listed in the Reference section of this paper.

For Forms authentication, this is enforced by the authentication provider.

### 11.300 (b) Password Policy

Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

**How Microsoft Windows and Active Directory addresses the requirement**

Windows and Active Directory infrastructure can enforce password policy for complexity and expiration. Windows integrated authentication and Basic authentication can leverage this automatically.

For detailed discussion as well as a step-by-step configuration guide of windows accounts and password policy, please refer to the articles listed in the Reference section of this paper.

A similar mechanism will need to be implemented by the authentication provider if Forms authentication is used.

### 11.300 (c) Deactivation of Users

Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

**How Office 2007 System addresses the requirement**

Windows and Active Directory administrators can deactivate users, change users passwords, or require users to change passwords after issuing a temporary password. Windows integrated authentication and Basic authentication can leverage this automatically.

These capabilities can be extended to Digital Signatures through Active Directory and the use of Microsoft Certificate LifeCycle Manager.

Similar mechanisms will need to be implemented by the authentication provider if Forms authentication is used.
**11.300 (d) Unauthorized use of passwords or identification codes**

Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report on an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

**How Office 2007 System addresses the requirement**

The Microsoft Windows family of products, including Microsoft Windows Server 2003, Windows Vista, and Windows XP can all audit logon changes and failed attempts.

Group policy can enforce account lockout policy to help to prevent brute force password guessing. Lockout policy is based on failed attempts for a time window and users can be locked out for specified times before they can attempt again (or not).

Group policy can also enforce password policy to mitigate the risk of unauthorized credential use. Password policy can be set to enforce complexity of the password (including minimal length and combinations), password aging (expiration), and password history (reuse of previous passwords).

Similar policies can be extended to Digital Certificates through the use of Microsoft Certificate Lifecycle Manager.

**11.300 (e) Identification Code Device Testing**

Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

**How Office 2007 System addresses the requirement**

This should be part of the operational procedure that is written into the compliance policies and procedures.
**Systems Validation and Compliance**

Systems validation and compliance is covered in depth in a Microsoft whitepaper entitled “Validation and the Microsoft Platform”.

This whitepaper covers the following topics:
- Microsoft software development practices and how they map to the industry “v-model”
- Installation Qualification methodology using Microsoft tools and system resources
- Operational Qualification methodology using Microsoft tools and system resources

This whitepaper will be available on MSDN at the Microsoft Life Sciences Developer Center (http://msdn.microsoft.com/lifesciences).
References
2007 Office System Document: Compliance Features in the 2007 Microsoft Office System

Regulatory Compliance Planning Guide

Office 2007 Planning Guide
http://www.microsoft.com/office/preview/beta/deploy.mspx

Step-by-Step Guide to Enforcing Strong Password Policies

Account Passwords and Policies