WHITE PAPER:
THE SYMANTEC FOUNDATION FOR
MICROSOFT SHAREPOINT® GOVERNANCE

The Symantec Foundation for Microsoft SharePoint® Governance

Who should read this paper

This white paper is designed to assist Microsoft SharePoint® administrators in developing a governance plan by leveraging the Symantec solutions for SharePoint.

Confidence in a connected world. Symantec.

Content

Introduction **1**

What is SharePoint Governance? **1**

Part 1—IT Governance **1**

Server centralization, consolidation, and migration **1**

Quotas and storage management **2**

Site lifecycle management **2**

Stage 1—Content is created 3

Stage 2—Content is moves to the archive and is replaced with a shortcut in SharePoint 3

Stage 3—Content is only available in the archive. 3

Stage 4—Deletion 4

Data protection **4**

Part 2—Information Management **5**

Records management and eDiscovery requirements **5**

Securing content and sites **6**

Optimizing search **6**

Conclusion **7**

Introduction

In his book “Mindsight," Daniel Siegel proposes that an optimal state exists somewhere between rigidity and chaos. Too much rigidity stifles creativity and too little results in chaos, making it impossible to accomplish anything. This is also true of your Microsoft SharePoint® environment. While employing governance is essential to control the chaos, you need to leave your end users with enough flexibility to really harness the power of the platform. For this reason, creating a governance plan is no easy task.

A recent Osterman survey shows that 39 percent of SharePoint implementations still don’t have a governance plan.[1] This is largely due to inadequate resources and limited SharePoint knowledge within IT. To overcome this problem, SharePoint administrators should seek out software solutions to assist in developing and enforcing their governance strategy.

True governance provides control over the environment and data within. The focus of this paper is to provide a checklist of areas you must consider when creating your SharePoint governance plan, strategies, and solutions to help you achieve success and how Symantec solutions for SharePoint can assist with your plan.

What is SharePoint Governance?

Microsoft breaks SharePoint governance into three sub-categories:

- **IT Governance**—Governance of the software/service you provide
- **Information Management**—Governance of the content/information
- **Application Management**—Governance of the custom solution that admins provide

Symantec solutions for SharePoint assist in the first two categories. The first section of this paper will provide an in-depth look at IT Governance and the second section will focus on Information Management. Symantec solutions don’t really play a role in the third pillar of Application Management.

Part 1—IT Governance

Proper IT Governance provides control over the services that you offer within SharePoint, management of servers within the farm, and control over SharePoint implementations within the organizations. A proper plan will include SLAs for backup and recovery with both a Recovery Time Objective (RTO) and Recovery Point Objective (RPO). It will also include plans to centralize the environment (for example, migrating many work group level implementations rolled into a single centralized implementation). IT Governance also includes security for the SharePoint farm.

Server centralization, consolidation, and migration

In most companies, SharePoint was initially adopted at the work group level to facilitate document sharing. Little thought was given to growth and management as the number of users was very small. As IT became more aware of the use of SharePoint within the organization, a more centralized approach was adopted, shifting work group level implementations to a single centralized environment.

One of the goals of IT Governance is to bring many disparate SharePoint implementations under a single centrally managed solution. This involves first having awareness and control over the implementations on your network and then moving to a single centralized farm. Related to consolidation is the need to migrate the farm to a new version of SharePoint as these tasks are often done at the same time. Symantec offers solutions to help with migration and consolidation of SharePoint servers.

1- Osterman Research, “Improving SharePoint Use and Governance,” October 2012.

One of the first steps in migrating or consolidating content is to decide what content needs to be moved to the new farm. Symantec™ Data Insight for SharePoint is a powerful tool to help make decisions on which content you should bring into the new environment. Data Insight provides analysis of your data to show which content is actually being accessed. If content hasn't been accessed in a few years, chances are it will not need to be moved into the new environment unless it must be kept for eDiscovery or regulatory purposes.

Symantec Enterprise Vault™ can further assist in a migration or consolidation. Older content can be archived and replaced with a shortcut to preserve the end-user experience. This can drastically reduce the size of the database. If 80 percent of content is older, a 10 TB database is suddenly reduced to 2 TB accelerating the migration and setting the new farm up for more efficient backup/recovery.

Symantec NetBackup™ can also play a role in consolidation efforts by allowing content to be backed up from one farm and restored to another at the Web application level. Symantec Backup Exec™ can also do this and can even redirect restores at the site level. This feature can be used to move content from a farm that will be retired to the new centralized farm.

Quotas and storage management

When setting up a new site, you may wish to implement quotas to help control storage moving forward with the new farm. Quotas can be set up at the site collection level and serve two purposes:

- Control storage bloat and reign in growth
- Educate end users on the need to delete content

SharePoint allows you to configure both warning and ultimate storage limits which cannot be exceeded. Quota templates can be created which can be applied to any site. When the warning limit is reached, the site administrator receives an email notification. When the quota limit is reached, the site collection goes into 'read-only' mode.

Enterprise Vault assists with keeping the site collection under the quota limit by replacing content with a 6 byte shortcut. When a quota warning limit is reached, a more aggressive archiving/shortcutting policy can be configured to keep within the ultimate quota limit. Enterprise Vault for SharePoint also assists by deleting active SharePoint content via "Deletion Rules." This allows content to be removed from SharePoint based on rules created within the Enterprise Vault for SharePoint policy. Rules can be based on file type (for example, delete all MP3 files), date (delete content that hasn't been modified in two years), or any other metadata value in SharePoint.

Another way to stay within quota limits is to manage SharePoint versioning, which is used to preserve changes to a document or item as the final document develops. Every change to the document is saved as a separate file within SharePoint 2007/2010, resulting in storage bloat. For example, if you modify a 5 MB PPT file to simply change the date, another 5 MB of storage is used in SharePoint. Storage can grow very rapidly when you consider all of the document libraries within your SharePoint environment. SharePoint 2013 introduces 'Shredded Storage' technology which helps to reduce overall storage but versioning still carries some overhead. Steps can be taken to limit the impact of versioning within SharePoint itself, such as reducing the number of document libraries and limiting how many versions are maintained. You can also setup retention stages to delete older versions after a period of time. Enterprise Vault for SharePoint allows you to preserve all versions but only keep the current version in SharePoint. All older versions are moved to the archive and replaced with a link to the archived version to preserve the end-user experience.

Site lifecycle management

One of the big challenges in SharePoint management is controlling how long data should live and the stages of the lifecycle. SharePoint provides tools for this, including retention stages which can automatically move content to different locations and ultimately delete the

content. Administrators can govern how sites are created, size, and longevity by using self-service site management and site use confirmation and deletion. Finally, implementation of expiration and access policies are proven ways to control content.

Enterprise Vault adds value to the native lifecycle management solutions by adding proactive archiving to capture critical content into the archive and thus enabling site expiration without fear of deleting a document that may be required due to regulations or for other reasons. Enterprise Vault also introduces a more granular lifecycle for content:

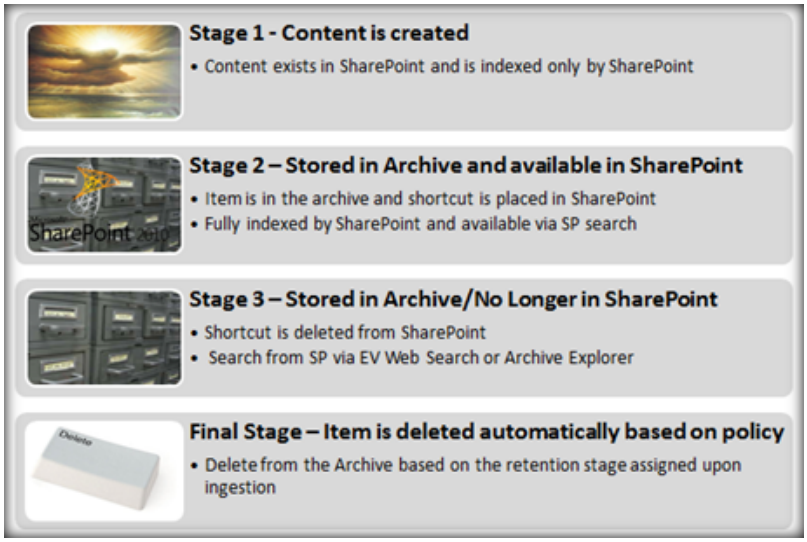

Figure 1. Content lifecycle with Enterprise Vault for SharePoint.

Stage 1—Content is created

When first created, content is stored directly in the SharePoint database providing fast access to content. Content can also be copied to the archive without replacing the original item in SharePoint as archiving and shortcutting are separate processes in Enterprise Vault for SharePoint. This allows content to be preserved (possibly on WORM storage) for compliance purposes while still maintaining optimal end-user access within SharePoint.

Stage 2—Content is moves to the archive and is replaced with a shortcut in SharePoint

In Stage 2, the item is no longer directly stored in SharePoint but instead now resides exclusively in the archive. To preserve the end-user experience, a shortcut replaces the original file within SharePoint. An end user may not even notice that the item resides in the archive as the icon and user experience does not change. Even the search experience is preserved and SharePoint will still fully index archived content as long as the shortcut is in place.

Stage 3—Content is only available in the archive

After a period of time, content ages and becomes less relevant to users and you may wish to delete the shortcut in SharePoint as this causes the item to no longer appear in search results and in the document library. Content can now only be found in the archive and by using the Enterprise Vault for SharePoint search Web part or other archive search tools, such as Archive Explorer. Customers should be trained to look for older items using these archive search tools as this point.

Stage 4—Deletion

The final stage in the lifecycle is actually deleting the content and this is the stage that is probably most important as content tends to live in SharePoint forever. Enterprise Vault assigns a retention category as the content comes in the archive which controls when the content will ultimately be deleted from the archive. Enterprise Vault 10.0.4 will add the ability to provide granular retention categories based on policy rules. This will allow content in the same location to have different retention categories or retentions assigned to specific people or groups if desired.

Another part of determining the proper content lifecycle is to find optimal storage for content at each stage. With Enterprise Vault you can assign retention to WORM storage, disk, tape, or even the cloud for content once it is archived. Data Insight also provides guidance on storage for SharePoint content. It provides a history of content access to alert you when content may be deleted (for example, if not accessed in six months). It can also highlight critical to ensure it is properly stored and protected. Data Insight also determines content ownership which may also assist in determining the importance of content (for example,content created by the CEO may need to be kept longer than content created by the mailroom attendant). This data can be used to determine optimal storage, define backup/recovery schedules, and archiving policy.

Data protection

Within Information Governance, data protection really refers to maintaining the integrity of the SharePoint environment. It covers providing a recovery policy In the event of a catastrophic failure of the SharePoint environment and will generally include commitments on services levels to restore access to the farm and the recover point for data within SharePoint.

Net Backup and Backup Exec offer complete disaster recovery for SharePoint and provides the ability to not only back up the underlying operating system but also the entire SharePoint farm. NetBackup will interrogate the front-end server to discover the other servers within the farm. If your SharePoint environment is completely virtualized, you can back up the entire farm by simply backing up the virtual machine images. This not only provides disaster recovery but allows content to be restored at any level. You may restore the entire farm, or a single Web application, site collection, document library, or even file or list item—all from the virtual machine backup. This greatly accelerates the process, as you only need one backup to provide disaster and granular recovery.

Data Insight could be used with NetBackup or Backup Exec to provide guidance on the most critical information in SharePoint based on usage. You could adjust your backup policy based on this information to ensure the most important databases are targeted with more aggressive backups to ensure a suitable Recovery Point Objective (RPO).

Enterprise Vault for SharePoint can optimize storage resulting in is a smaller database size and greater ability to quickly backup/recovery current SharePoint content. If 90 percent of content is older and not frequently accessed, archiving, and replacing with a shortcut could reduce a 20 TB SharePoint environment down to about 2 TB. This dramatically improves your ability to back up your current content and reduces the storage needed for daily/weekly backups.

Once content is archived it still needs to be protected, however archived content can be moved to a closed partition within Enterprise Vault after reaching a specified size. Once in a closed partition, content really won't change so frequent backups are unnecessary. Typically, a closed partition can be backed up once per quarter. If 90 percent of your content can be moved to the archive and only backed-up once per quarter, not only do you save time but also gain very significant savings in backup storage media.

Part 2—Information Management

Information Management concentrates on the management and protection of content generated and stored within SharePoint. Certain verticals are subject to strict regulations about the creation and capture of electronic communications—proper Information Management will take this into consideration and plan accordingly. Sensitive data is often shared within SharePoint and must be strictly controlled to ensure that the people who can access this content are those who should have access. Finally, Information Management is focused on the protection of this content from deletion if relevant or required for long-term storage.

Archiving and eDiscovery play a big role in proper Information Management. A proactive archiving solution not only protects data, it also may be required to ensure proper compliance to regulations such as those facing financial services and other highly regulated industries. Without a proper eDisovery solution, litigation results in a firedrill where terabytes of data must be examined to determine the megabytes that may be relevant to a case.

Records management and eDiscovery requirements

More mission-critical content is moving into SharePoint. This includes corporate records which need to be preserved and may be discoverable. Most regulated companies understand the need to capture and discover email, but they often overlook the risks associated with SharePoint. This is changing. As SharePoint is more widely utilized, the need to capture and discover the content becomes more necessary. SharePoint itself may be considered a data custodian in many organizations. Many financial service firms are unable to completely take advantage of their SharePoint implementation unless they have the ability to retain content for compliance reasons.

eDiscovery of SharePoint can be done proactively via archiving or reactively via direct discovery from live SharePoint data. Both are valid, provided that the content can be protected against modification or deletion and that the metadata remains intact during collection. Proactive archiving has the added benefit of moving content out of the production environment to optimize storage and protect data against being destroyed by users or via system failure. It also avoids the fire drill of enforcing a legal hold against live data from multiple sources in the event of litigation. It can also accelerate eDiscovery by providing a single repository to search against all content sources including email and files. Enterprise Vault for SharePoint provides proactive archiving.

Reactive discovery is useful to capture the latest content from the live environment. Unlike archiving, it doesn't provide the storage optimization benefits and there would need to be greater reliance on the basic retention capabilities within SharePoint (retention stages, in-place hold). Companies may wish to employ a hybrid approach where certain sites/libraries which may contain sensitive data are proactively archived and less critical data and all other content will rely on reactive discovery.

To identify content that is relevant to a case, you will need to perform keyword searches of the content and you will also need to filter based on the custodians involved, date range, and content sources. You may also wish to filter based on custom metadata within SharePoint. As mentioned above, many large companies have terabytes of data to sort through so accurate filtering is essential to minimize the downstream review process.

Once content has been identified as relevant to a case, the content must be preserved. Content that is proactively archived can be placed on hold in the archive to supersede any assigned retention category and prevent the content from being destroyed. If you are leveraging a reactive approach, you will need to leverage the hold capabilities within SharePoint and the legal hold module of Clearwell for notification.

SharePoint 2013 provides a basic tool called eDiscovery Center in SharePoint 2013 (SharePoint 2010 has a more limited keyword search capability). This solution is limited to searching content, placing it on hold, and exporting it. The eDiscovery Center does not offer robust filtering and review capabilities required to manage large volumes of data found in today's SharePoint farms.

Symantec™ eDiscovery Platform powered by Clearwell™ can ingest content directly from SharePoint and also archived SharePoint content from Enterprise Vault. It provides advanced filtering capabilities to allow users to find the content they are looking for quickly. Tools such as predicative coding, advanced metadata search, keyword proximity, and filter-based refinement of results can greatly accelerate the process of finding relevant content. Symantec eDiscovery Platform also provides tools to redact content that is not relevant to the case and may be sensitive.

Securing content and sites

Security around specific content is often overlooked in the rush to create new sites and share content. Far too often content is shared with a broader audience than intended and inappropriate access can result. Special care must be given to sites which contain corporate assets and personally identifiable information. Content access should be audited for this type of content and steps taken to ensure the information is protected. This may lead to special permissions for sites, sub-sites, or even a specific site collection.

You must also consider the need for external access. Companies may have a need for partners or even customers to access portions of their SharePoint environment. This adds another level of complexity and concern when planning your SharePoint farm and governance plan.

Symantec provides several solutions to help protect against inappropriate access.

Data Insight for SharePoint provides data activity reports and monitoring alerts. It provides tools to investigate and solve data breaches and provides a complete audit of who accessed sensitive content within SharePoint. Data Insight can be used to find open sites and data at greatest risk for exposure and can provide guidance on steps to address this leakage.

Symantec™ Data Loss Prevention also scans content for sensitive information based on rules, regular expressions, templates (for example, a company contract), and other criteria. When it finds content that may be sensitive and is not properly protected with suitable access restrictions, the content can be quarantined until such time as the weaknesses can be addressed.

Symantec protection for SharePoint provides malware and antivirus protection by scanning both on upload/download and background scans of the database.

Optimizing search

Not finding what you are looking for in a timely manner is one of the biggest complaints from SharePoint end users. As SharePoint farms grow to multiple terabytes in size, this complaint will only get worse. Microsoft has improved search greatly with SharePoint 2013 by blending the best features of the fast engine into the SharePoint search engine. This includes advanced features such as visual and text based "best bets," which return a defined result to match a specific search query. Phonetic searches are also leveraged so that a search for "Tom Smyth" might also provide results for "Thom Smith."

Companies are also improving search results by forcing the capture of detailed metadata and training users to use advance search leveraging metadata values such as created/modified date. Another decision with your new governance plan is to decide on which content should be indexed and what should not. Data Insight could assist with this by identifying content that is rarely accessed and then removing it from the SharePoint index.

Even with these improvements, the problem of finding the needle in the haystack can still persist. The best way to address this issue is to have a clear plan to move content out of SharePoint as it ages and becomes less relevant. As discussed in the lifecycle section, Enterprise Vault provides the ability to enforce a lifecycle and ultimately move old content exclusively to the archive before ultimately deleting it in an effort to keep SharePoint search results relevant.

Conclusion

SharePoint governance is essential but difficult to implement and must be done in a way that doesn't tie the hands of the ultimate users of SharePoint. With proper tools, you can effectively manage the environment (IT Governance) and manage your data effectively (Information Management) with minimal impact on end users.

The Symantec solutions for SharePoint can greatly improve your odds for success:

- Enterprise Vault for SharePoint will help to provide IT Governance by immediately relieving storage costs via archiving. It will control growth leading to efficient backup/recovery and better performance with no end user impact.
- The Symantec eDiscovery Platform solution provides the ability to quickly review content and features transparent predictive coding which leverages machine learning technology in order to assist with review workflows to dramatically reduce review time. It provides both direct collection from SharePoint and direct collection from all archived content within Enterprise Vault.
- NetBackup can efficiently backup the entire farm and provide both disaster and granular recovery from a virtual machine image.
- Data Loss Prevention identifies and can even quarantine content that has inadequate protection.
- Data Insight provide details on what content is being used, content that can be deleted, and the proper ownership of content within your SharePoint environment.

Leveraging solutions such as these will dramatically improve your ability to rein in your SharePoint environment and ensure a well-managed environment for the future.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
6/2013 21300644