Governance – SharePoint Server 2010

Concepts

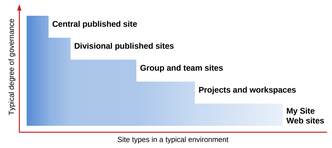
Governance Areas

Governance is the set of policies, roles, responsibilities, and processes that guides, directs, and controls how an organization's business divisions and IT teams cooperate to achieve business goals.

Three major areas for governing SharePoint 2010 Products:

- IT governance of the software itself and the services you provide
- Application governance of the custom solutions you provide
- Information Management governance of the content and information that users store in those services.

Governance and Site Types



Different types of sites frequently require different governance policies.

Typically, published sites have tighter governance over information and application management than team sites and My Site Web sites.

Each type of site should have a specific IT Service plan, so that the service level agreements match the importance of the site to the organization as a whole.

Governance Stakeholders

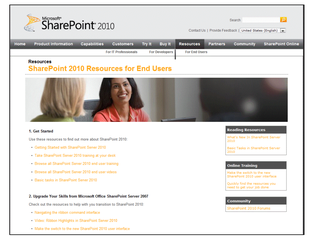
You must ensure that your governance policies are appropriate to your organization's goals, and you must keep them up-to-date as business needs change. Form and use a governance group to create and maintain the policies and include the following roles:

- Information architects or taxonomists
- Compliance officers
- Influential information workers
- IT technical specialists
- Development leaders
- Trainers
- IT managers
- Business division leaders
- Financial stakeholders
- Executive stakeholders

Governance and Training

Governance doesn't work without user adoption and compliance.

End-user training and education, good content, and search are keys to user adoption.



IT Governance

For IT governance, you can control the services that you offer, and you can control or track software installations in your environment to prevent proliferation of unmanaged servers for which you can't provide support. What will you provide with each service, and what will you include in service-level agreements for each service?

IT service governance

When you develop an IT service to support SharePoint 2010 Products, a key to success is your enterprise's ability to govern the service and ensure that it meets the business needs of your organization in a secure and cost-effective way. A successful IT service includes the following elements:

- A governing group defines the initial offerings of the service, defines the service's ongoing policies, and meets regularly to evaluate success.
- The policies you develop are communicated to your enterprise and are enforced.
- Users are encouraged to use the service and not create their own solutions – installations are tracked and rogue installations are blocked.
- Multiple services are offered to meet different needs in your organization. Offering a set of services enables you to apply unique governance rules and policies at various levels and costs. In addition, you can phase in services in a manageable way.

What to govern:

- Quotas – Quota templates define how much data can be stored in a site collection and the maximum size of uploaded files. Associate different quota templates with site collections at different service levels.
- Site lifecycle management – You can govern how sites are created, the size of sites, and the longevity of sites by using self-service site management and site use confirmation and deletion. Set expiration and access policies to control content in sites.
- Asset classification – Classify sites and content by value and impact of the content to the organization (such as high, medium, or low business value/impact). Classification then controls other behaviors, such as requiring encryption for high business impact information.

Impact = Exposure	**Value = Availability**
If this leaks, will it hurt my business?	If this isn't available, can my business run?

- Data protection (backup and recovery) – Vary the level of data protection that you offer based on service levels. Plan the frequency at which you back up the farms and the response time that you will guarantee for restoring data.
- Security, infrastructure, and Web application policies – how is the system and infrastructure maintained and who has access at what levels. Are you controlling use of fine-grained permissions?

Service-level agreements should include:

- Length of time and approvals necessary to create a site.
- Costs for users/departments.
- Operations-level agreement – which teams perform which operations and how frequently.
- Policies around problem resolution through a help desk.
- Negotiated performance targets for first load of a site, subsequent loads, and performance at remote locations.
- Recovery, load balancing, and failover strategies.
- Customization policies.
- Storage limits for content and sites.
- How to handle inactive or stale sites.
- Multi-language support.

Deployment governance

In addition to governing services that you offer, you also need to govern installations of SharePoint 2010 products in your environment. You can block all installations, or track and monitor installations. And you should make sure that your installations have the current software updates installed.

Block installations

You can block installations of SharePoint 2010 Products to prevent users from installing them to unauthorized servers that you cannot support. You use a group policy in Active Directory Domain Services (AD DS) to set a registry key on all servers that block installations.

Keep current with software updates

Always keep your servers current with the latest software updates. For more information, see the Updates for SharePoint 2010 Products Resource Center at http://go.microsoft.com/fwlink/?LinkID=160585.

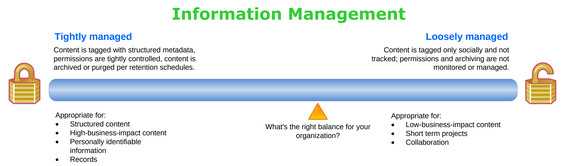
Track installations

An Active Directory Domain Services (AD DS) marker named Service Connection Point identifies the SharePoint 2010 Products servers in an organization. To use this marker, create a container in AD DS and set the permissions for the container before you install any SharePoint 2010 Products in the environment. Then, when you or another user in your domain runs the SharePoint Products Configuration Wizard as part of installing SharePoint Server 2010, this marker is set and can be tracked by using AD DS. You must set this marker for each domain in your organization if you want to track installations in all domains. This marker is removed from AD DS when the last server is removed from a farm.

Microsoft® SharePoint® Server 2010

Information Management

Information management is the governance of information in an enterprise — its documents, lists, Web sites, and Web pages — to maximize the information's usability and manageability. Another aspect of information management is determining who has access to what content – how are you making content available internally and externally and to whom?



Information architecture

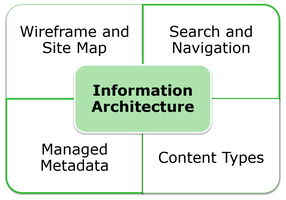
Information architecture determines how the information in that site or solution – its Web pages, documents, lists, and data – is organized and presented to the site's users. Information architecture is often recorded as a hierarchical list of content, search keywords, data types, and other concepts.

Good information architecture supports the following goals:

- Manageability: can the IT team effectively implement and manage the information?
- Requirements: does the information architecture meet regulatory requirements, privacy needs, and security goals?
- Business: does the architecture add to your organization's effectiveness?

Questions to ask when designing a site or solution:

- How will the site or solution be structured and divided into a set of site collections and sites?
- How will data be presented?
- How will site users navigate?
- How will search be configured and optimized?
- Is there content you specifically want to include or exclude from search?
- What types of content will live on sites?
- How will content be tagged and how will metadata be managed?
- Does any of the content on the sites have unique security needs?
- What is the authoritative source for terms?
- How will information be targeted at specific audiences?
- Do you need to have language- or product-specific versions of your sites?



Integrate your information architecture with your environment's search strategy. Take advantage of Enterprise search features like best bets, people search, and content sources and connectors for external content.

Information access

Be sure to consider access to content when you design your solution and sites. This overlaps with IT Governance as you consider your entire environment. Ask the following questions:

Information Management: Permissions and Audiences	**IT Governance: Access**
How do I structure permissions in a site? How do I target content to specific audiences? Should I use Information Rights Management (IRM) to protect content?	How do I make this content accessible to external users? How do I make sure that only people who need access have it?

Information management tools

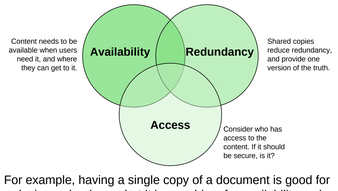
Govern your content by using tools for content management, including:

- Use workflows and approval for document centers and site pages – wherever official documentation is stored.
- Use approval for published Web sites to control pages.
- Use version history and version control to maintain a history and master document.
- Use content types with auditing and expiration for document libraries to manage document lifecycle.
- Manage uploads to large libraries by using the Content Organizer.
- Use site use confirmation and deletion to manage site collection lifecycles.
- Identify important corporate assets and any sites that contain personally identifiable information – be sure that they are properly secured and audited.
- Use Records Centers to store, audit, and control records in compliance with regulations or laws.

Determine the rules or policies that you need to have in place for the following types of items:

- Pages
- Lists
- Documents
- Records
- Rich media
- Blogs and Wikis
- Anonymous comments
- Anonymous access
- Terms and term sets
- External data

When thinking about content, consider the balance between the following factors. Which of these factors is the highest priority for each type of content?



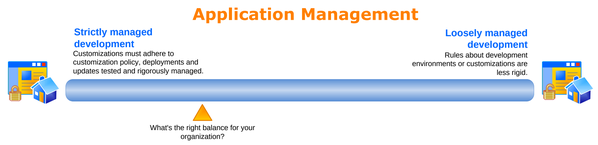
For example, having a single copy of a document is good for reducing redundancy, but it is a problem for availability and access if it is deleted.

Map out the preferred content lifecycle. What steps need to happen when a list item, document, or page is created, updated, or deleted? For best results, develop a long term rather than a temporary solution.

Much of this should be covered by your document and records management plans, but also consider the storage costs for the content. Understand the capacity planning limits for documents and items, and keep performance and scale in mind.

Application Management

How will you manage the applications that are developed for your environment? What customizations do you allow in your applications, and what are your processes for managing those applications?



Customization policy

Determine which types of customizations you want to allow/disallow, and how you will manage customizations. Your customization policy should include:

- Service level descriptions
- Processes for analyzing customizations
- Process for piloting and testing customizations
- Guidelines for packaging and deploying customizations
- Guidelines for updating customizations
- Approved tools for development
- Who is responsible for ongoing code support
- Specific policies regarding each potential type of customization, whether the customization is code-based or no-code (done through the user interface or SharePoint Designer)

Sandboxed solutions

Consider using a restricted execution environment, called a sandbox, to isolate custom solutions. Sandboxed solutions cannot use certain computer and network resources and cannot access content outside the site collection they are deployed in. Sandboxed solutions can be deployed by a site collection administrator. Only a farm administrator can promote a sandboxed solution to run directly on the farm, outside its sandbox, in full trust.

Branding

Consistent branding with a corporate style guide makes for more cohesive-looking sites and easier development. Store approved master pages in site galleries for consistency so that users will know when they visit the site that they are in the right place. Define which parts of the template can be changed by site owners and which cannot. Allow room for sub-branding of individual team or project brands.

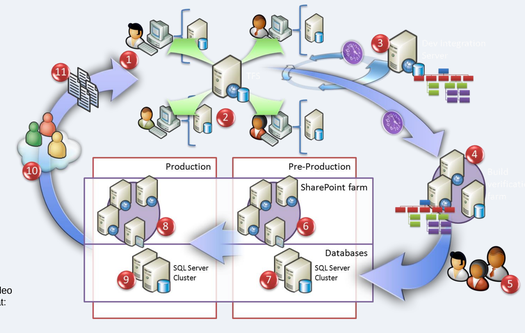
Lifecycle management

Follow these best practices to manage applications that are based on SharePoint 2010 Products throughout their lifecycle:

- Use separate development, pre-production, and production environments (see Deployment model) and keep these environments in sync.
- Test all customizations before releasing initially and after any updates have been made before you release them to your production environment.
- Use source code control and solution and feature versioning to track changes to code.

Summary of lifecycle management process

1. Initial requirements are gathered and tasks assigned.
2. Developers use tools to track development and store source code for customizations.
3. Automated builds are generated for integration testing.
4. Build verification farm is used for additional testing (larger environments).
5. Testing personnel test the customizations.
6. After testing, customizations are deployed to pre-production environment.
7. Pre-production environment matches production environment as closely as possible.
8. After verifying in pre-production, customizations are deployed to production.
9. Previous testing ensures that when customizations are deployed to production, there are no unexpected issues or problems encountered.
10. End users use the production environment, provide additional feedback and ideas. Issues are reported and tracked.
11. Feedback and issues are transformed to requirements and tasks, cycle begins again.



For a full explanation of this process, see the video **Development Lifecycle for SharePoint 2010** at: http://go.microsoft.com/fwlink/?LinkId=200174.

Microsoft®