

Five Steps to Embed Compliance in SharePoint

By David Gwyn, Vice President R&D and Collaboration, HighPoint Solutions

In highly regulated industries, organizations often turn to enterprise content management systems like Documentum that are built to cope with stringent controls, audits and regulations, despite costs and maintenance requirements which exceed those of SharePoint. Most firms assume compliance cannot be embedded into SharePoint since the platform allows for constant changes and evolutions from end users without involving IT. However, new tools and processes being leveraged in the life sciences industry point to ways companies can constrain SharePoint to achieve compliance.

1. Establish a comprehensive information architecture. Information architecture is a conceptual model that illustrates how information is labeled, organized and made available. It is as critical to the deployment and use of SharePoint as it is to traditional content management solutions. Since SharePoint is designed to be a viral platform that is not completely within the IT group's control, standards must be established and enforced to achieve business goals. This important requirement is often overlooked.

Traditional system designs focused on document taxonomy and metadata, which define how documents will be classified and tagged. A more complete SharePoint model includes:

- ◆ Site hierarchy;
- ◆ Navigation;
- ◆ Look and feel;
- ◆ Content lifecycle management;
- ◆ Personalized content; and
- ◆ Content types and metadata.

2. Embed repeatable, secure processes with stringent workflows. Business processes that ensure compliance can be built into SharePoint through several mechanisms. One example is Nintex Workflow, which provides a drag-and-drop graphical tool for creating workflow steps. Not only does the graphical model encourage broader use, but select components or entire workflows can be reused, allowing firms to establish consistent methods for managing the content lifecycle and controlling approval processes.

Furthermore, Nintex Workflow offers the capability to extend the platform to external partners by automating the addition of users to the Active Directory and establishing

appropriate security models. It can also be leveraged to support approval workflows for site creation, which addresses one of the more difficult areas to manage within SharePoint.

3. Enable digital signatures. Many industries have been leveraging the value of electronic signatures for years, e.g. for signing an email or entering an ID and password to authenticate an approval, but a digital signature is the only legally binding method in the electronic world. It not only provides the ability to sign the document, but also securely seals it against changes.

ARX CoSign adds digital signature capabilities that can be embedded within a SharePoint/Nintex workflow. The combination of SharePoint, Nintex and ARX expands collaborative possibilities well beyond traditional content management solutions. External parties can be sent documents to digitally sign through workflows that automatically provision the credentials without the need for IT support.

4. Institute auditing capabilities to deliver the evidence required by government agencies. Answering the question of "Who's been doing what to my SharePoint content?" is managed through the configuration of audit settings. These settings allow SharePoint to track user activity in a secure repository that includes not only behaviors such as check-in and check-out, but also activities such as viewing or downloading content.

Additionally, the use of tools such as Axceler's ControlPoint software provides the ability to audit your SharePoint site to analyze user permissions at any point in the SharePoint farm, even down to the document level.

5. Develop a proper governance structure. Since SharePoint is typically not locked down and the structure can be changed by many users, a governance structure is necessary to ensure that the compliant processes you implement with workflows and digital signatures remain that way. In more traditional content management systems, the deployment and use of the system was controlled by the system architecture. Content was organized in folders and the cabinet/folder hierarchy was typically



David Gwyn

David Gwyn is vice president of R&D and collaboration for HighPoint Solutions. With more than 20 years of experience in the life sciences industry, Gwyn is a seasoned executive with extensive skill in delivering Documentum and SharePoint. He is a member of the Project Management Institute, International Institute of Business Analysis and the Drug Information Association.

controlled by IT, thus providing a virtual vaccine against the viral spread of an uncontrolled taxonomy.

Since SharePoint is designed to reduce the need for IT involvement and put more control in the hands of end-users, procedural controls must be established to ensure that the proliferation of sites, libraries and folders does not reach pandemic proportions. This is managed through an effective, multi-tiered governance structure that provides guidelines and scope at each level to provide boundaries on end-user creativity. These levels often are segmented at the farm, site-collection and site tiers, with each level building details on the decisions made in the tier above.

Prove it Through Validation

By defining a robust information architecture that defines what and how content is stored and the ways in which it can be found, users are more likely to follow procedures and use the system as intended. By leveraging powerful workflow tools and digital signatures that actually improve the business process, activities are controlled and streamlined in a manner that offers value to the business community, rather than constraining it. By configuring SharePoint to capture these activities in the audit log and establish appropriate layers of governance to review and monitor usage, the necessary controls and safeguards are put in place.

A question that Microsoft is constantly addressing is: "Can SharePoint be validated?" While the answer to this question is clearly "yes," many still question how it is achieved. By utilizing a risk-based approach and following the steps above, one can clearly show that major risks have been mitigated and addressed. ■

HighPoint Solutions is a premier provider of specialized IT and consulting services for the life sciences and healthcare industries. Additional information is available at www.highpoint-solutions.com.