WHITE PAPER

SharePoint Governance: Do Something or Do Nothing?

An Osterman Research White Paper

Published March 2013

SPONSORED BY

actiance®

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

Microsoft SharePoint is becoming a critical part of many organizations' information management environment and, as such, must be managed properly and in accordance with corporate governance and compliance mandates that may be driven by particular industries, jurisdictions, legal precedent, corporate culture, and other factors. However, while SharePoint is a robust offering with a wide range of capabilities, it lacks some important features that prevent organizations from fully maximizing its benefits.

Fundamentally, this white paper takes the position that managing SharePoint effectively is even more urgent when using it for information management tasks that are subject to strict regulatory, legal or best practice requirements, and that its native capabilities are insufficient to meet all of an organization's corporate governance obligations.

KEY TAKEAWAYS

- SharePoint is used for a variety of information management tasks, the majority of which are subject to regulatory, e-Discovery, and legal mandates, as well as existing corporate policies. Organizations that use SharePoint for information management, but ignore these wider requirements, are exposing themselves to significant and unnecessary risk.

- Managing SharePoint properly – through both governance processes and technology-enablement – offers significant advantages. These include corporate risk mitigation and lower lifecycle cost for SharePoint in light of brand, reputational, and legal costs for failing to address these risks.

- Technology to enforce appropriate corporate policies and to adhere to regulatory and legal obligations must include three core capabilities: policy-driven, granular capture of content; real-time alerting to ensure that policy violations are detected and remediated as soon as possible; and contextual capture of information.

- Getting started with managing SharePoint properly is a four-step process: assessing the risks that apply to a particular organization, developing detailed and granular corporate policies, deploying technology to enable the enforcement of these policies, and reviewing the policies frequently in light of changing regulatory, legal, and corporate requirements.

ABOUT THIS WHITE PAPER

This white paper focuses on the compliance aspects of SharePoint and why it is important to incorporate complementary technologies that augment its native functionality. The paper also provides a brief overview of Actiance, the sponsor of this document, and its Vantage offering that provides compliance and management features not available natively in SharePoint.

The Growing Importance of Microsoft SharePoint

THE GROWING USE OF SHAREPOINT

Over the past decade, organizations have been moving an increasing number of collaboration and information management tasks over to SharePoint, usually starting with intranet publishing or team collaboration tasks before incorporating other SharePoint features. Microsoft's vision of

an integrated information management platform is becoming a reality for organizations of all sizes and across all industries. The growing adoption of SharePoint is best illustrated by the following data points:

- Among all of Microsoft's server offerings, SharePoint achieved $1 billion in annual revenue in the shortest amount of time.
- 20,000 new SharePoint users are added every day.
- Organizations pay between $6 and $9 to channel partners and consulting firms for every $1 in licensing fees they pay to Microsoft.

The bottom line is that SharePoint has been successful for Microsoft, its business partners, and the organizations that have opted to make it a central part of their collaboration and content management capabilities.

WHAT SHAREPOINT DOES

Although it is the focal point in Microsoft's strategy for unstructured business information, SharePoint does not stand alone. It integrates with several other services from Microsoft in order to bring a comprehensive set of features to the organization:

- Microsoft Exchange integration provides a mechanism for email messages to be automatically routed into pre-specified locations within SharePoint. Email messages can then be shared among a team, including managing the records within them.
- Microsoft Outlook integration provides a way for employees to work with specific SharePoint content, alongside their email, tasks, and calendars. Team-level information can be viewed in the context of personal information.
- Microsoft Lync integration brings the presence and availability information from Lync to SharePoint. Business users can see whether their colleagues are available from the SharePoint interface and can initiate text, voice, and video conversations directly from SharePoint.
- Microsoft Live Meeting integration means users can conduct shared-screen meetings with one or more colleagues, enabling all parties to see the same information at the same time. Real-time joint editing capabilities streamline revision cycles and eliminate unnecessary travel.
- Information in SharePoint is stored in Microsoft SQL Server, enabling massive scalability, as well as the opportunity to leverage Microsoft's database investments. Essentially, SQL Server and SharePoint enhancements go hand-in-hand.
- Access and authentication information is mastered in Microsoft Active Directory and is leveraged by SharePoint to reduce the costs and risks of identity management.

- SharePoint doesn't just integrate with other Microsoft products: there are connectors for SAP, Lotus Notes, and Documentum, among many others.

WHAT SHAREPOINT DOES NOT DO

While SharePoint offers a range of important features and functions, there are a number of critical features that are not native to the product. These include real-time alerts when sensitive, confidential, or damaging content is posted by SharePoint users; granular capture of content based on specific corporate, regulatory, or other governance requirements; contextual capture of content so that information can be presented with other relevant content, such as during e-Discovery; the provision of role-based reviewer workflow capabilities; the ability to tightly control user access to various types of SharePoint content; and the ability to create highly granular policies to meet specific organizational policy requirements. In short, SharePoint is a robust offering but cannot satisfy the full range of an organization's corporate governance requirements.

Corporate Governance is Critical for SharePoint

In light of the essential corporate information stored in most Microsoft SharePoint environments, it should be clear that SharePoint must be treated in accordance with corporate governance best practices. Corporate information must be managed properly for a variety of reasons, those being regulatory compliance, e-Discovery, legal holds, and adherence to corporate policies. Let's consider each in turn.

REGULATORY COMPLIANCE

First, corporate information must be managed for regulatory compliance purposes. Many organizations operate under specific regulatory regimes, and these mandate particular approaches for corporate information. For example:

- Sarbanes-Oxley sets out the particular controls required for dealing with financial information and applies at a supra-industry level.

- The Health Insurance Portability and Accountability Act (HIPAA) establishes various rules for handling and securing healthcare information regarding Protected Health Information. Ensuring privacy and confidentiality of patient health information is a primary focus of HIPAA but has been expanded in recent years to include a wide range of firms that deal with healthcare providers, benefits administrators, and others.

- The Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) set standards and requirements for firms operating in the securities industry in order to prevent fraud and other financial wrongdoing. Certain types of information must be retained for set periods of time, and information must be sampled to ensure compliance with regulatory obligations.

- Rule 26 in the FRCP (Federal Rules of Civil Procedure) sets requirements for discovery and production of documents, email messages (and attachments), video files, and other electronically stored information for civil litigation in federal court cases. Rule 34 mandates a timeframe for production of such information, as well as specific provisions for privileged

information.

- Data breach notification laws require that government agencies, businesses, and individuals that store personal information on a computer system advise the individuals concerned if the data has been, or is believed to have been, accessed by unauthorized parties. A data breach is typically defined quite broadly by these laws, encompassing everything from a hacker's attack, in which information is stolen, to a missing backup tape that contains unencrypted information.

- Organizations doing business outside of the United States will almost certainly be subject to local market regulations in the legal jurisdictions in which they operate. A common example is the strict data privacy laws in Europe and the United Kingdom.

e-DISCOVERY

e-Discovery requirements cover the breadth of electronic communications and document storage and are an important factor when it comes to managing corporate information. In litigation, an organization must comply with discovery requests from lawyers for documents (including spreadsheets and slide decks), email messages, conversation threads, and other information that may highlight what happened at some point in the past. Companies are given a set timeframe in which they must respond or face financial penalties or legal consequences. Even if this information has been archived off the production SharePoint environment, it must still be discoverable. Because of the emphasis on tracing responsibility and establishing cause in litigation, a detailed audit log showing who created and accessed the various documents and other information is essential. To minimize the financial impact of e-Discovery, it is important that the right amount of information be retained – not too much so as to drive up legal costs, and not too little so as to create the risk of spoliation of evidence. Moreover, information should be presented with correlating data to give meaning and context to the findings.

LEGAL HOLDS

Another important aspect of corporate governance in a SharePoint environment is to support the requirements of legal holds. Given the nature of the information being stored, it is almost certain that a portion of this will be covered by a legal hold at some point in the future. This means that due to litigation against the organization – or even when management suspects that such an action is imminent – action must be taken to ensure that potentially relevant information is not be deleted, even if it is scheduled to be deleted in line with the company's records management policy. Multiple legal holds can be in place at any one time, each covering the same documents and records. There is a legal requirement – backed up by stringent penalties – for documents and records under such a hold to be retained until otherwise notified.

CORPORATE POLICY COMPLIANCE

Finally, compliance with corporate policies should be a driving factor in establishing corporate governance in SharePoint environments. Organizations are extremely protective of their intellectual property and have strict policies, as well as strong technologies, in place to protect against this type of loss. These policies need to be enforced in SharePoint, with specific actions taken to restrict access, protect against unauthorized external access, and limit what can happen with sensitive material that is created and stored– even after it has been removed from SharePoint. Well-governed organizations also have corporate policies in place to protect against data breaches, to prevent creation of certain types of data, and to stop inappropriate content

from being created or transmitted. In an ideal system, notification of any breaches, posting of inappropriate content, etc., are managed in real-time in order to minimize corporate risk. These corporate policies have implications on how organizations approach SharePoint given their compliance requirements.

CONSEQUENCES FOR FAILING TO MANAGE SHAREPOINT

In light of the above reasons for the proper management of corporate information, it is clear that there are significant consequences for failing to manage information properly. These include:

- Brand damage and the consequential drop in market valuation as customers, investors, and governments lower their perception of an organization's governance competence.
- Reputational damage, as customers are less inclined to do business with a firm with a poor history of governance over sensitive information, particularly if this has impacted customers directly.
- Legal consequences, as customers initiate litigation to shield themselves from the consequences of poor information management practices.
- Regulatory penalties for failing to comply with mandatory industry regulations, as we have outlined above.
- Potential to lose business, as customers take their business to other vendors that have demonstrated greater competence in appropriately managing information.
- Long-term consequences, such as the reduced ability to attract and retain top employees.

In summary, there are important reasons why SharePoint must be governed in line with wider corporate governance mandates and significant consequences of failing to do so.

To Manage SharePoint or Not

Organizations must choose between two options: To Do Nothing or To Do Something. Let's look at both options.

DO NOTHING

The default option is to do nothing – to leave SharePoint to become whatever it becomes, with no oversight, control, or governance. This approach is inexpensive in the short term and requires little effort with regard to understanding the risks of SharePoint from a governance perspective. The only actions required are to purchase the technology and let it run.

However, the simplicity and low expense of the "do nothing" approach quickly gives way to enormous risks. At a technical level, these include poor search results for employees, extra storage hardware to handle the ensuing document load, and a growing sense of user confusion about how SharePoint actually makes a positive difference. These are but the tip of the iceberg though, as the business risks are much more severe: the increased probability of legal troubles,

running afoul of regulatory requirements, questions over business continuity, the possibility of loss of business as customers shift their relationships to other vendors with a lower risk profile; an inability to detect when policy violations have occurred; and an inability to manage policies at a sufficiently granular level.

DO SOMETHING

The second option is to do something – to manage SharePoint properly and to make the requisite investments of time, effort, and money. This approach – or the consequences thereof – includes having to pay money for consulting services and add-on tools to make governance work properly, as well as the need for a clear strategy as to what SharePoint should become and the actions required to get there. In order to transform SharePoint into a productive asset for the organization, investment of some sort, whether it's defining the strategy for its use or investing in additional solutions, is necessary.

The benefits of the "do something" approach are unequivocal:

- Corporate risks are dramatically lowered, along with the costs associated with being in violation of these particular areas.

- Concerns regarding regulatory compliance diminish as the organization makes a substantive effort to understand the regulations with which they need to comply, given their unique business model and geographical focus areas.

- An approach to addressing these issues within SharePoint can be developed in advance of any problems arising, thereby demonstrating good corporate governance and reducing the risk of being hit with a punitive fine.

- The ability to quickly and efficiently comply with e-Discovery requests is enhanced, due to the implementation of an information management framework that takes a comprehensive inventory of SharePoint's holdings.

- Documents and other information covered by an e-Discovery request can be quickly located, without requiring substantial financial and physical investments.

- The same can be said of the organization's ability to comply with legal holds – an approach is proactively in place to ensure that relevant information is properly managed during one or more legal holds.

- Finally, the risk of being out-of-step with current corporate policies is significantly reduced. Policies that address information management requirements, protect intellectual property, and ensure appropriate security can be interpreted within the SharePoint context.

In summary, all organizations must a) pay the cost for managing SharePoint properly by managing it proactively and thereby reaping the benefits associated with sound information management and corporate governance practices; or b) pay for it reactively, after significant problems rear their heads and the very foundation of the organization is threatened.

MANAGING SHAREPOINT PROPERLY

Management of SharePoint in light of regulatory, legal, and corporate mandates can be summarized into three core capabilities. In other words, while there are multiple drivers for managing SharePoint, they coalesce into three specific technical capabilities:

- **Granular capture of content**
  Policies for the capture of SharePoint content must be defined at a global level, but also in a much more granular fashion for groups and for individual users, so that corporate governance, compliance, legal, and other standards can be fully satisfied. From a compliance standpoint, granular policy definition and content capture is critical in order to satisfy the myriad regulatory and records management requirements of Sarbanes-Oxley, HIPAA, SEC, FINRA, IIROC, FSA, FERC, and other requirements, as necessary. However, granular policy and capture can also reduce storage costs by eliminating the capture of unnecessary content, expedite e-Discovery efforts by minimizing the amount of reviewable content, and minimize corporate risk by retaining only relevant content.

- **Real-time alerts for potential policy violations**
  The ability to provide real-time alerts can prevent the publication and distribution of content that might be harmful to an organization, such as offensive language, confidential intellectual property, financial statements, draft policy documents, and other sensitive or confidential information. Real-time alerts based on content detection are essential to preventing data leaks, loss of corporate reputation, regulatory violations, and legal risks.

- **Contextual capture of content**
  Another critical capability is the capture of information in its appropriate context, such as the presentation of related or linked items in the same user interface. Contextual capture is invaluable during e-Discovery, early case assessments, or even informal management reviews of information. Moreover, capture of information in context can substantially reduce the costs of litigation, minimize the potential for failing to produce information due to simple oversight, and limit the likelihood of sanctions arising from production delays. This capability is particularly important when responding to e-Discovery and related requests, given the relatively tight timeframes for responding to various discovery-related requests in many jurisdictions.

Next Steps

Organizations looking to establish a framework for managing SharePoint should start with four steps.

STEP 1: UNDERSTAND THE RISKS

Corporate policies and technology selection should happen after a detailed analysis of the specific and particular risks faced by an organization, if they choose not to manage SharePoint use. While we have outlined some of the known risks in this white paper, most decision makers require specifics related to their organization, not generalizations. Which of the risks discussed apply to your unique situation? What regulations govern your specific industry? How do these requirements change in light of new statutes and interpretations by regulators and the courts?

A discussion with your in-house general counsel is a prudent place to start. He or she should have a good sense of what does and does not apply.

STEP 2: DEVELOP DETAILED AND GRANULAR CORPORATE POLICIES

Policies set a shared expectation for what should happen under particular circumstances. Policies should communicate the why (the reasoning and logic behind the policy), the what (the actions that are supposed to happen or those that are not supposed to happen), and the consequences of failing to abide by the policy. Specific, clear, and unambiguous details are essential for an effective policy; otherwise, its application is left up to individual judgment, resulting in continual escalation about specific instances.

STEP 3: DEPLOY TECHNOLOGIES THAT WILL ENABLE POLICY ENFORCEMENT

Source and implement technology that enables the practical enforcement of corporate policies on a day-to-day basis. Training and education are instrumental in making policies work, but these are insufficient without technical enforcement. Technology that enforces policies ensures consistency of action, reminds employees of the standards, and significantly reduces the risk that policies will be ignored or forgotten in the usual course of business.

STEP 4: REVISIT POLICIES FREQUENTLY

Finally, new regulations, legal precedents, and changes in corporate goals will demand a revision of corporate policies from time to time. The implications of a changing environment on existing policies should be considered regularly – if not continually – and current policies should be updated, removed, or superseded as needed. Making employees comply with policies that are no longer necessary, as well as failing to make them comply with new regulatory, legal, or corporate requirements, are reflective of an insufficient governance process. The idea is governance, not govern-once.

Summary

SharePoint is emerging as the dominant platform for various information management and collaboration roles in organizations today. It has the capabilities to support team collaboration, document management, business intelligence, and more. With this emerging role comes the responsibility to face up to the risks of using SharePoint for storing information that is likely to be covered by industry regulations, e-discovery and legal hold demands, and corporate policies. Failing to take specific steps to manage SharePoint properly is very risky, and while it saves money in the short term, is likely to result in severe costs and consequences in the future.

Osterman Research believes that all organizations using SharePoint to store and provide access to corporate information must manage SharePoint in light of the specific risks being faced. This will entail understanding those risks, developing specific corporate policies, and implementing technology to enforce those policies over time. Ensuring that policies remain in lockstep with a changing regulatory, legal, and corporate agenda is also essential.

Vantage

Vantage is the de facto platform for granular security and policy controls for real-time communications – providing management for the broadest set of applications and modalities, including Microsoft Lync and SharePoint, public instant messaging platforms such as Windows Live Messenger and Skype, Web conferencing, and industry-focused networks like Thomson Reuters Messenger, Bloomberg, and YellowJacket.

About Actiance

Actiance® is a global leader in communication, collaboration, and social media governance for the enterprise. Its governance platform is used by millions of professionals across dozens of industries. With the power of communication, collaboration, and social media at their fingertips, Actiance helps professionals everywhere to engage with customers and colleagues so they can unleash social business.

The Actiance platform gives organizations the ability to ensure compliance for all their communications channels. It provides real-time content monitoring, centralized policy management, contextual capture of content and smart archiving which improves the efficiency and cost-effectiveness of eDiscovery and helps protect users from malware and accidental or malicious leakage of information. Actiance supports all leading social media, unified communications, collaboration, and IM platforms, including Facebook (FB), LinkedIn (LNKD), Twitter, Google (GOOG), Yahoo! (YHOO), Skype, IBM, (IBM), Jive (JIVE), Microsoft (MSFT), Cisco (CSCO), and Salesforce.com (CRM).

Actiance is headquartered in Belmont, California.

In the USA:
Toll-free: +1 888 349 3223
Phone: +1 650 631 6300
Fax: +1 650 598 2820
info@actiance.com
www.actiance.com

For Web and Unified Communications security news, follow Actiance on Twitter, http://www.twitter.com/actiance