AvePoint DocAve White Paper

Migrate. Integrate. Manage. Optimize. Protect. Report.

# Meeting Compliance Objectives in Microsoft® SharePoint®

## Balancing Access, Security, and Data Protection

**Dana Simberkoff**

# NOTICES PAGE

# Contents

# The Compliance Landscape

Senior executives today are faced with a formidable challenge in managing their IT environments: juggling competing requirements for collaboration and participation; the explosion of big data and unstructured content; and the need for increased compliance. Enterprise Content Management (ECM) systems like Microsoft SharePoint have exponentially increased the amount of content available and accessable on internet, extranet, and intranet sites. They enable employees to collaborate better, interact on demand, integrate "social" into their work environments, and respond more quickly to customer needs. They form the backbone of the new social media phenomenon, which has firmly taken root in the culture of modern society. While these ECM systems truly help organizations meet their business needs and have firmly entrenched themselves into the company DNA, they have also created an explosion of new content.

## More Content, Greater Risk

Every employee within a company is now a "content contributor." This business reality brings new risks to the forefront, and enterprise organizations are subsequently facing the pressure of meeting increasing regulatory, statutory, and organizational compliance mandates . Traditional Compliance Officers (Chief Privacy Officers, Chief Information Security Officers, Records Managers, and Legal Staff) are struggling to address this new level of risk. New disciplines, such as Governance, Risk, and Compliance (GRC), have developed to respond to these needs.

Mistakes, particularly those caused by employees, represent the largest "perceived" risk in the compliance arena. The Society of Corporate Compliance and Ethics and Health Care Compliance Association conducted a survey in January 2011 to both identify compliance officers' areas of responsibility as well as their assessment of the risk. The survey found that fears of an accidental breach far outweigh fears of an intentional breach. Respondents were asked how likely they felt that data would be released through hacking attacks; intentional breaches by employees and third-party vendors; and accidental breaches by employees and vendors. In general, the feeling was that accidental breaches were far more likely. To sum up the findings:

- Just 8% felt that it was somewhat or very likely a hacker would gain access to the system
- 61% thought an accidental breach by employees was somewhat or very likely
- Only 30% thought an intentional breach by employees was likely
- 41% thought an accidental breach by a vendor was somewhat or very likely
- Only 13% thought an intentional breach by a vendor was somewhat or very likely

These findings show that concerns over an accidental breach, whether carried out by employees or third-party vendors, were far more substantial than concerns over intentional attacks. As such, organizations must ensure that compliance guidelines for data access, transfer, and management are well documented and clearly communicated to ensure that employees and vendors alike can verify their actions against organizational rules and regulations. Making compliance ubiquitous throughout the

organization – and as automated as possible – is the preferred approach to further reducing the risk of an accidental breach.

## The Heavy Cost of Accidental Data Breaches: The Reality

It is certainly tempting to think that accidental breaches, while being the forefront fear for any compliance officer, won't happen to your company. Unfortunately, the reality of these breaches could easily turn into a nightmare of litigation and continuous class action suits. A number of high-profile cases has resulted from exactly these types of lapses in data security compliance, including:

- April 2011 – In what many are calling the largest breach of data security in modern history, Sony Computer Entertainment, Inc., a subsidiary of Sony Corporation (together "Sony"), announced a massive data breach arising from theft by hackers of the Sony Playstation® Network, Sony Entertainment Online, and Sony Pictures, resulting in the compromise of the credit and debit card data of up to 100 million users involving more than 12 million cards in addition to service outage for more than 30 days. Sony estimated that breach remediation measures alone would cost at least $171 million, and no fewer than 55 punative class actions were filed against Sony in the United States and another three such actions were filed in Canada.

- October 2011 – Proving that break-ins are certainly a form of accidental data security breach, Sutter Health ("Sutter") announced the compromise of more than four million of its patients' data. The breach occurred after a computer containing *unencrypted* medical and personal information about millions of Sutter patients was stolen from Sutter's administrative offices in Sacramento, California.

  Class action complaints were filed on behalf of Sutter's patients. As outlined on the complaint, the security breach violated California's Medical Information Act because patients' health information was left unsecured and unencrypted in the stolen computer. If the class action suit is successful, Sutter may be obligated to pay up to $1,000 for each patient whose privacy was compromised. If approved, this amount could add up to anywhere from $944 million to $4.25 billion, not counting attorney fees and court costs.

  Given that the breach involved more than 500 people, Sutter was required to issue a press release which revealed there were two types of data stored on the stolen computer:

  1. A Sutter Physician Services database, which revealed the names, addresses, dates of birth, phone numbers, email addresses, medical record numbers, and the names of health insurance plans of more than 3.3 million patients stored in excess of 15 years; and

  2. A Sutter Medical Foundation database, which revealed the dates of services and medical diagnoses used for almost one million patients over a six-year period.

  Sutter claimed that the stolen computer was scheduled to be encrypted, but was stolen before action could be taken.

- June 2012 – LinkedIn Corp. recently announced that it had failed to take adequate security measures to protect confidential user data, resulting in a data breach via attack by hackers who stole an as yet to be determined amount of user data – at minimum including up to *6 million* user passwords. While the loss of passwords may seem a relatively minor issue, a number of suits have already been filed, including a pending class-action suit seeking recompense of up to $5 million. One of the determining factors in the size of the ultimate reward, if any, is whether or not other user information – such as emails – was stolen. If the theft was limited to passwords, the chances of success on the class-action scale is reduced dramatically, but is that a risk you're willing to take?

## Addressing Risk in Microsoft SharePoint 2010

SharePoint 2010 continues to achieve new milestones in the ECM and collaboration space. According to AIIM's 2011 "State of the ECM Industry" report, SharePoint adoption has been rapid with only 20% of organizations surveyed having no interest in SharePoint and close to 60% of respondents using it now. When looking at the largest organizations surveyed, 70% were using SharePoint. When AIIM looked at the SharePoint market specifically in its 2011 "Using SharePoint for ECM" report, it discovered that 53% of respondents consider SharePoint their primary ECM system going forward, with many companies achieving "near universal employee access". However, in spite of this, more than 60% of organizations have yet to incorporate their SharePoint deployment with existing compliance policies. Consequently, SharePoint is now a treasure trove of potentially sensitive and unprotected information within many enterprise organizations.

Compliance Officers are concerned with the risk created by SharePoint's "social" features because of privacy issues, inappropriate content, Personally Identifiable Information (PII), and potential exposure of protected content or sensitive information. This risk carries through to document libraries; collaboration sites; and of course Intranet, Extranet, and ECM sites, too. Ensuring that SharePoint deployments – and the vast, dynamic repository of content and communications managed through them – are in compliance with statutory, regulatory, and/or organization specific requirements necessitates a multi-prong approach which encompasses employee education, training, and awareness along with technical enforcement. Access and Rights Management Controls and monitoring, as well as change configuration management and audits, can lead to a more secure and less vulnerable environment. The ability to provide improved security of, and confidence in, SharePoint as a system for managing sensitive data has a positive impact on more than simply regulatory compliance and the protection of sensitive information – it is integral to SharePoint adoption.

## Aligning Compliance Initiatives with SharePoint Governance Policies

Compliance concerns and regulations should be considered and incorporated into any comprehensive governance model. Microsoft defines governance as " 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." With any site or solution that is delivered to the business through SharePoint, organizations have a choice to make that determines the level of governance that specific site or solution requires. It is important to note that this level of governance, however, is not solely up to the organization to determine. Depending on the nature of the content, regulations and mandates

may require very stringent governance controls for access rights, auditing, and content retention. So as you can see, governance policies for various sites and content must always account for the compliance regulations to which content is subjected, tying the two very closely together.

# Mandates and the Regulatory Framework

With regard to statutory requirements, there are hundreds of laws, mandates, and requirements that regulate protection of information[i]. Worldwide, Public Sector organizations, public companies, regulated industries, and even small-and-midsized businesses may be subject to a range of privacy and information security requirements. Privacy[ii] is a major concern of any organization that handles PII or protected health information (PHI). Corporations and government agencies are also concerned with data and information security with the goal of protecting confidential information such as corporate trade secrets and merger and acquisition information. In the military, there are concerns over the protection of operational security information, which includes protected military intelligence such as the movement of troops and naval operations. Many of these organizations have a need to separate sensitive content from non-sensitive content, and protected information or employees from their general populations. As evidenced in the selection of the aforementioned data breach litigation beginning on Page 4 of this paper, this is a very real threat to every company – not just those specializing in PII or PHI. A fundamental tenant of almost all compliance programs is the principle that private or sensitive information must be available only to people that have a right to access it and must be protected from those who do not. In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."[1] The seven principles governing the OECD's recommendations for protection of personal data were:

1. **Notice:** Data subjects should be given notice when their data is being collected.
2. **Purpose:** Data should only be used for the purpose stated and not for any other purposes.
3. **Consent:** Data should not be disclosed without the data subject's consent.
4. **Security:** Collected data should be kept secure from any potential abuses.
5. **Disclosure:** Data subjects should be informed as to who is collecting their data.
6. **Access:** Data subjects should be allowed to access their data and make corrections to any inaccurate data.
7. **Accountability:** Data subjects should have a method available to them to hold data collectors accountable for following the above principles.

[1] http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html

Critical factors for organizations to consider when managing risks to online document collaboration include:

- ✓ Balancing accessibility and security
- ✓ Classification of documents
- ✓ Confidentiality of documents
- ✓ Integrity of information within documents
- ✓ Understanding different roles

Organizations using SharePoint must find ways to safely balance the need to collaborate and share information with regulatory requirements and management of sensitive data.

# Enforcing SharePoint Compliance

When determining the best approach to implement and enforce compliance initiatives, Chief Privacy Officers, Chief Information Security Officers, Compliance Managers, Records Managers, SharePoint Administrators, and company executives will all have to work together to establish the most appropriate processes for their organization as well as an action plan for how to execute these processes. As with any process that governs how persons interact with technology, with regard to SharePoint there is a spectrum of how automated the process can be. Manual processes might involve more man power, lots of documentation and, as with any manually intensive process, may be prone to human error. Fully automating processes, however, means trusting the technology and often requires us to be able to audit any action technology solutions take on SharePoint environments and assets.

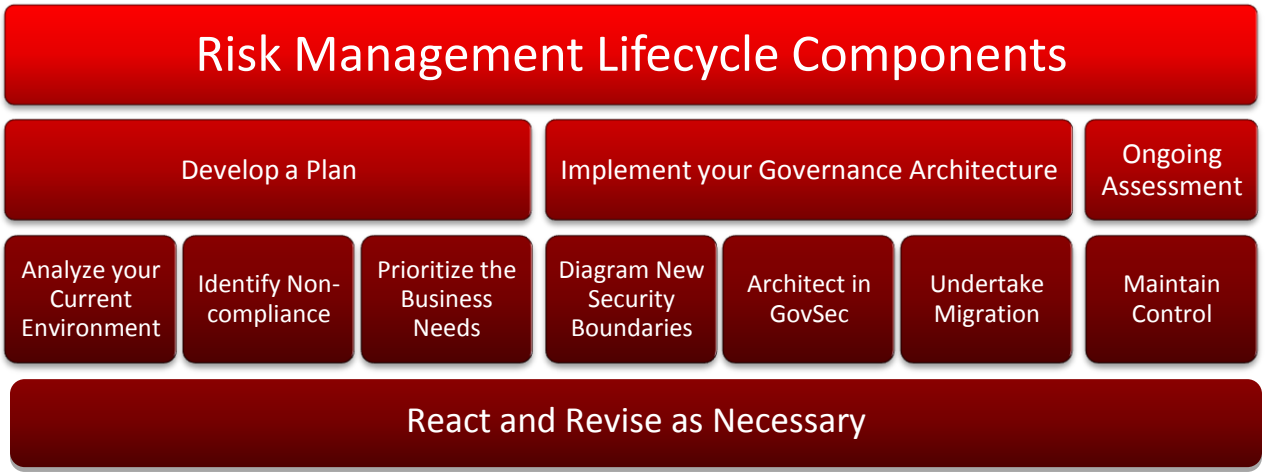
Technology solutions can be incorporated into overall compliance processes to allow the implementation of automated access and content controls for enterprise-wide SharePoint systems, enabling key stakeholders to understand how their SharePoint sites are being used and subsequently establish appropriate controls to maximize efficiency and access while also helping to prevent breaches. If and when a breach does occur, solutions – whether manual or automated – must allow the appropriate personnel to swiftly detect those breaches, track, respond, and recover. This mitigates the likelihood of a catastrophic incident, such as those experienced by Sony, Sutter Health, and LinkedIn, in addition to countless thousands of smaller companies worldwide. It will also help to gather information to perpetuate system hardening and improvements for the continuous life cycle that must make up a successful risk management program. This life cycle includes the following important components:

- **Develop a Plan:** Perform a site assessment, set your organization's goals, and establish appropriate compliance and governance requirements and standards.
- **Implement your Governance Architecture:** Technical enforcement and monitoring of your policy is critical, as is implementing training for employees that addresses areas of non-compliance.

- **Ongoing Assessment:** The adage, "You can't manage what you can't measure," rings true here as well. Conduct ongoing testing, monitoring, and assessment to ensure that you have complied with your new guidelines and standards.
- **React and Revise as Necessary:** Evaluate results; automate verification of guidelines and standards; and modify the program as necessary.

# Establishing Compliance Solution Requirements

Now that we've established lifecycle steps that are required for successful risk management, we can begin to establish requirements for compliance solutions that support each of the key components. For instance, to first establish a plan for risk management, organizations must gather insight into existing SharePoint assets as well as an understanding of what areas of SharePoint are currently subjecting the organization to the greatest risk. Without this initial intelligence and identification, compliance plans fail to address key areas of concern. As we continue to break down each of the lifecycle components, we're able to establish more granular technology requirements as diagrammed below.




The table below further details each of the aforementioned components of a successful risk management lifecycle program.

| | |
|---|---|
| **Analyze your Current Environment** | Analyze the current environment to determine the "compliance health" of a SharePoint deployment. Relevant information may include the topology of your SharePoint environment; a report of users, administrators, and their access controls and permissions; information about content that is being collected in your sites; and information about SharePoint usage data storage and capacity. |
| **Identify Non-compliance** | As your organization strives to understand and improve its current compliance posture, the need to audit environment health and risk periodically is essential in order to gain insight into risks of exposed PII, PHI, and inadequate access controls. |

| | |
|---|---|
| **Prioritize the Business Needs** | Implement an effective and realistic compliance program that can be enforced, measured, and modified as needed. Identify what data your organization collects, processes, and stores as well as from where it originates. Decide on applicable and/or mandatory privacy and security requirements – the what, where, why, and how. Provide information classification based on risk exposure to the organization, and define minimum content and physical security access controls based on risk classification. |
| **Diagram New Security Boundaries and Architect in GovSec** | Empower an organization's experts and/or policy managers to define policies; assign appropriate permissions and access to both protected and non-protected areas of their SharePoint sites; and provide access to sensitive content that is based on the content itself and/or user credentials. Implement the new security and data protection framework. |
| **Undertake Migration** | Move your existing content into the new "compliant environment". |
| **Maintain Control** | Continually monitor your SharePoint compliance health, as compliance is not merely a one-time event – rather, it is an ongoing process. Organizations must be able to make adjustments as needed to balance compliance, access, and optimal SharePoint performance. |

# An Introduction to AvePoint Compliance Solutions

AvePoint's Compliance Solutions address and support these six requirements with a multi-faceted approach encompassing automated assessment and technical enforcement of compliance requirements, to implement a truly effective risk management program lifecycle. AvePoint Compliance Solutions help organizations with the "discovery process" to understand the current state of affairs, producing reports with actionable insight to help establish appropriate data governance and compliance policies that reflect the priorities of the business as well as implement practices, procedures, and protection. The table below outlines how AvePoint Compliance solutions directly address each of the six requirements.

<table>
<tr><td rowspan="3">Develop a Plan</td><td>Analyze your Current Environment</td><td rowspan="3">Evaluate the existing SharePoint infrastructure through a risk assessment framework, including a full-featured reporting platform that identifies single points of failure, potential "bottlenecks", security risks & risk related to capacity in order to help organizations ensure their initiatives are in-line with governance policies.<br><br>Reports and analytics include:<br><br>• User permission, configuration, settings report<br>• Compliance reporting (audit records of users, content)<br>• PII scan, based on AvePoint and client specifications and classifications<br>• Usage analytics, CPU, and topology reports</td></tr>
<tr><td>Identify Non-compliance</td></tr>
<tr><td>Prioritize the Business Needs</td></tr>
</table>

| | | |
|---|---|---|
| **Implement your Governance Architecture** | **Diagram New Security Boundaries and Architect in GovSec** | • Empower an organizations' experts, policy managers, and content owners to assign appropriate permissions to their SharePoint sites, ensuring that information managed through SharePoint is available and accessable to the people who should have it and protected from the people who should not.<br>• Easily configure deployment-wide access controls and configurations in batch-mode at any object level, an organization's risk of breach and site/content sprawl remains in check. |
| | **Undertake Migration** | Compliance Officers can implement automated access and content controls for their enterprise-wide SharePoint systems (and file share systems), by:<br>• Exposing existing file share content in SharePoint<br>• By migrating existing enterprise-wide content into SharePoint |
| **Ongoing Assessment** | **Maintain Control** | AvePoint Compliance Solutions help to maintain control by providing organizations with the ability to continuously monitor and enforce access controls and necessary configurations at any level and in batch mode. |

With these capabilities, AvePoint Compliance Solutoins enable Compliance Officers to understand how their SharePoint sites are being used and put controls in place to maximize efficiency and access while also helping to prevent breaches from happening. However, if and when a breach does occur, AvePoint solutions also allow the appropriate personnel to swiftly detect those breaches, track, respond and recover. This not only significantly lessens the likelihood of a catastrophic incident, but also helps to provide information back to the organization that can allow the proper stakeholders to harden the system and improve the continuous risk management program lifecycle. AvePoint Compliance Solutions enable organizations to experience cost savings while mitigating risk and supporting compliance.

# Functional Benefits

By supporting the six compliance solution requirements, AvePoint's Compliance Solutions capabilities are able to help organizations continuously gather information and perpetuate system hardening and improvements through the best-practice risk management lifecycle approach, preventing breaches before they occur, or detecting, tracking, and responding and resolving breaches as they occur. At any stage in this risk management lifecycle, AvePoint Compliance Solutoins are able to assess environments, allowing organzations to improve process and policies along the way. AvePoint Compliance Solutions provide "Access and Rights Management" controls, user and content lifecycle reporting, and continuous monitoring. These can all lead to a more secure, more accessible, and less vulnerable environment. With these capabilities, organizations are able to streamline how they prevent, detect, track, and respond to and resolve compliance infractions.


Specific features that assist with each step of the risk management lifecycle are outlined in the table below:

| Lifecycle Step | AvePoint Compliance Solution Capabilities | |
|---|---|---|
| | **Overview** | **Features** |
| **Prevent** | Proactive policy enforcement prevents users from being able to perform incorrect actions in the first place. | • Allow users to provision secure and non-secure sites based on "who they are" or the group of which they are a member<br>• Restrict SharePoint administrator privileges, allowing administrators to manage specfic areas of SharePoint<br>• Manage all user permissions granularly and in batch mode to prevent unauthorized access to content<br>• Assign metadata and restrict access to sensitive content with real-time filtering and scheduling<br>• Assign policy access rights to content stored on file shares<br>• Scan, flag and/or block all sensitive or offending content prior to upload |
| **Detect** | If and when a compliance infraction occurs, AvePoint Compliance Solutions enable quick detection of the event. | • Detect and make changes to content and/or user permissions and access that violate organizational-specific policies<br>• Proactively discover and block offending content via real-time scan, or run a scheduled risk report<br>• Search for user permissions – security search individual user or group profile of security permissions – and make requisite modifications on-demand |
| **Track** | Complete your investigation determining who, what, when, where, | • Record, monitor, and analyze SharePoint events and activity via automated reports<br>• Track user activity with the user life cycle report to see who did what, when, and where |

| | | |
|---|---|---|
| | why and how the breach occurred. | • Track content life cycle (what happened to the content) item life cycle reports |
| **Respond & Resolve** | AvePoint Compliance Solutions enable organizations to quickly take corrective action by implementing a legal hold; archiving or removing content from an unprotected area; or restructuring permissions and access to prevent the likelihood of a repeated breach. | • Respond and resolve infractions from one central interface<br>• Retain all SharePoint content in immutable form for compliance purposes<br>• Search for and provide legal hold and tracking of any content that breaks a pre-defined policy<br>• Provide true archiving and encryption of content<br>• Set up user permissions for compliance groups to investigate and act upon affected content<br>• Prevent future unauthorized access by adjusting security permissions and content access policies with swift permissions or content restructuring capabilities that preserve metadata |

This continuous life cycle of risk mitigation allows this information to be fed back into your "prevention strategies". Taking these precautions proactively will go a long way in ensuring that your company doesn't experience catastrophic remediation costs should a breach occur. Data breaches can happen at any time: The more AvePoint can help you in protecting your company, the less likely you'll be on the drafting end of a press release as to why your company now owes members billions of dollars as a result of data breach.

To learn more about AvePoint Compliance Solutions, please visit us on the Web:
http://www.avepoint.com/sharepoint-solutions/compliance

[i] There are a wide range of regulatory and statutory requirements that AvePoint supports for our regulated customers. These include for example: Statutory Requirements; HIPAA/HITECH Act, The Privacy Act of 1974, Section 208 of the E-Government Act, The Federal Information Security Management Act,Platform for Privacy Preferences (P3P) requirements, Children's Online Privacy Protection Act (COPPA), Gramm-Leach Bliley Act (GLBA), DoD OPSEC Requirements; Records Management Requirements, Dod 5015.2, Sarbanes Oxley; FINRA requirements-Financial Industry Regulatory Authority, Many regional specific data protection and privacy mandates for example:European Union Data Protection Directive, Asia Pacific Privacy Framework, Personal Information Protection and Electronic Documents Act (abbreviated PIPEDA or PIPED Act))-Canada

[ii] AvePoint is a corporate member of the International Association of Privacy Professionals (IAPP)