Compliance Healthcheck
For Microsoft® SharePoint®

Assess & Detect	Report	Strategize	Respond & Resolve

In today's marketplace, almost every employee is now a content contributor. This influx of new content, however, brings about new risks: Legal systems worldwide are clamping down and demanding greater compliance, particularly on IT systems, making it essential that organizations quickly implement compliance and risk management protocols. As Microsoft® SharePoint® continues to expand its footprint as an industry leading enterprise content management (ECM) and collaboration platform, it is imperative that enterprises align their SharePoint farms with existing compliance policies. Compliance officers are concerned with the risk created by SharePoint's features including MySites, Team Sites, and Wikis, as well as other more widely used features such as document libraries and ECM sites. These key elements of SharePoint potentially expose sensitive personally identifiable information (PII), classified information, or otherwise non-compliant content.

The Compliance Healthcheck for Microsoft® SharePoint® provides organizations with an as-is assessment of a select portion of their SharePoint environment, detecting any areas of concern or risk, and delivers a comprehensive report to key stakeholders, including compliance officers, agency executives, and administrators, raising awareness of compliance infractions or at-risk sites. After the assessment is delivered, organizations will be presented with best practices and proven approaches to subsequently reduce the risk of compliance infractions, and will be able to utilize AvePoint's best of breed Compliance Solutions to automate policy implementation and enforcement.

Key Challenges

1	2	3	4
Comprehensively assessing the as-is risk of SharePoint sites and file shares, detecting content/user access that can potentially violate your compliance policy to help establish compliance and governance standards	Producing a comprehensive report that can be distributed to compliance officers, administrators, and content owners that identifies the current risk levels associated with the as-is state of the SharePoint environment	Developing a comprehensive risk management plan that implements governance architecture with technical enforcement to prevent breaches by quickly identifying sensitive and/or classified content leaks and misuse	Quickly and efficiently reacting to a security breach or content contamination by swiftly quarantining detrimental data and easily restructuring security settings and permissions

Compliance Healthcheck for Microsoft® SharePoint®

Assess & Detect "As-is" SharePoint Compliance	Report on Compliance Infractions	Develop a Comprehensive Risk Management Strategy	Respond & Resolve Compliance Breaches
• Perform risk analysis and trend data to monitor and understand exposure levels for a defined scope of SharePoint content, as well as the effectiveness of existing controls to determine the overall "heat map" of an existing SharePoint environment • Generate detailed risk-level reports of content containing sensitive data including PII and PHI,to locate offending content, informing organizations where the majority of non-compliant or sensitive content is stored • Determine the nature of existing sensitive or non-compliant data by scanning against pre-configured or customizable dictionaries	• Report on user and content permissions, and manage individual user or group profile security settings • Identify data leakages or risk-defined content • Utilize filtered audit reports to identify the exposure and activity of site collections, or individual documents that contain sensitive information • Track all user and group activity with real-time or scheduled reports to determine origins of compliance infractions and users who have accessed this content	• Design an information architecture to address compliance and governance requirements for all SharePoint and network content • Determine appropriate permissions and security settings based on the governance and compliance requirements of SharePoint or file-based information • Strictly regulate user-generated content to prevent the creation or uploading of non-compliant, harmful content	• Determine a best practices approach for remediation of any identified compliance issues • Prioritize recommended changes to streamline the future implementation of a restructured compliance framework • Easily audit security settings, investigate usage patterns, and monitor sensitive information to assess the effectiveness of the risk management strategy • Generate and view reports with various attributes such as time viewed, deleted, renamed, and modified

This analysis identifies not only the existence of sensitive data, but also uncovers other key factors about the data, the SharePoint users and the system itself, including the nature of the sensitive (or non-compliance data), where it's located, its age, who created it, and who's accessed it. With these findings, our teams will then recommend a best practices approach to remediate any compliance issues, allowing the business to prioritize issues and implement a restructured compliance framework.

For organizations looking to move forward with an automated approach to manage risk in SharePoint, AvePoint Compliance Solutions enable automated access and content controls for enterprise-wide SharePoint systems (and file share systems) to prevent, detect, and respond and resolve to breaches. AvePoint helps to mitigate the likelihood of a catastrophic incident, and feeds back information that will lead to system hardening and improvements for the continuous life cycle that must make up a successful risk management program.

Next Steps

If you would like a solution demonstration, or to receive pricing information, please contact: ComplianceSolution@avepoint.com, or your Microsoft or TSP representative.

Accessible content available upon request.