Cloud Readiness Assessment
For Microsoft® SharePoint®
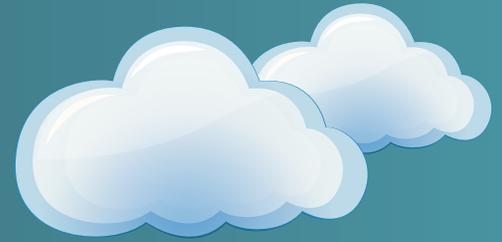
Assess	Classify	Restructure	Migrate

Organizations worldwide are quickly adopting cloud computing in order to stay ahead of a hyper-competitive business landscape. The immediate draw to cloud computing is clear – reduced total cost of ownership and less hardware for IT administrators to maintain. Hosting Microsoft SharePoint through Microsoft Office 365 could reduce cost and improve global access to SharePoint content. However, for organizations subject to regulatory requirements, the move to the cloud is not without risk. Enterprises have significant concerns about storing business data outside the walls of their enterprises, due to non-employee IT administrators possessing a high level of access and control over information; available technology options to secure and manage user access and authentication; or even intentional or accidental actions of employees or contractors. Furthermore, compliance officers are concerned with the risk created by SharePoint's "social" features – including MySites, Team Sites, and Wikis – as well as other more widely used features such as document libraries and ECM sites, which potentially expose sensitive personally identifiable information (PII), classified information, or otherwise non-compliant content. To overcome these concerns, organizations can opt to offload select content or workloads to the cloud, and keep their most regulated content on-premises.

To allow organizations to gain value from cloud computing initiatives while addressing compliance concerns, AvePoint and Microsoft have teamed up to deliver the Cloud Readiness Assessment. Through this assessment, organizations are able to identify sensitive or regulated content and notify key stakeholders including compliance officers, company executives, and administrators of any at-risk content. Once the initial assessment is complete, a best practices approach is outlined to separate regulated and non-regulated content or workloads, and subsequently migrate appropriate content to the cloud.

Key Challenges

1

Developing a comprehensive assessment to identify at-risk content or data breaches, including SharePoint or file share content/user access that can potentially violate your compliance policy

2

Implementing governance architecture with technical enforcement to efficiently tag, classify, quarantine, or delete sensitive or non-compliance content to support information management requirements

3

Establishing a desired information architecture for content, applying appropriate permissions, tags, and security settings to address compliance and governance requirements and standards

4

Quickly and efficiently migrating appropriate workloads or content to the Cloud to lower TCO and begin taking advantage of Cloud Computing

AvePoint® **Compliance Solutions** for Microsoft® SharePoint®

Assess Existing Sites and Content	Report on and Classify Content	Design Compliant Information Architecture	Determine Cloud Migration Approach
• 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 with configurable scans for violations out of the box (e.g. 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	• Record all infractions details, user interactions, security changes, and search queries on the specified content scope • 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	• Recommend a best practice approach to safely expose, access, and manage all content residing in the network and/or the cloud to SharePoint for centralized document management based on unique business requirements • Define requirements for restructuring permissions, and adjusting access, metadata and security settings of SharePoint content • Strictly regulate user-generated content to prevent the creation or uploading of non-compliant, harmful content	• Utilize content and site assessment reports and subsequent tagging to develop a best-practice approach to migrating select content and workloads to the cloud • Identify cloud-appropriate content for migration with customizable filters based on metadata or content types • Determine migration schedules and project milestones to ensure content is migrated to the cloud according to business need, allowing for roll-out to end users as business needs dictate • Propose a schedule for ongoing risk trend analysis reports to monitor and understand exposure levels and whether the existing controls are working appropriately

For organizations looking to implement the assessment recommendations, AvePoint Compliance Solutions can automate the classification, restructuring, and migration of content. In addition, AvePoint's Compliance Solutions can be utilized to automate access and content controls for enterprise-wide SharePoint systems (and file share systems) to prevent breaches and mitigate the likelihood of a catastrophic incident, while feeding 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 to receive pricing information, please contact ComplianceSolution@avepoint.com, or your Microsoft or TSP representative.