Managing Compliance Risk in SharePoint®

1 IDENTIFY RED FLAG RISKS

Identify Risks: Identify compliance risks, content, locations, accessibility, permissions, etc.

2 ESTABLISH THE COMPLIANCE STRATEGY

Determine what areas of risk to address and align with the business strategy. Use stakeholder knowledge to define the policies and procedures for the organization against the business strategy.

3 DESIGN POLICIES & DEPLOY

Design Policies: Define policies, business requirements, policy officers, appropriate actions, restricted access rules, notifications and workflows using HiSoftware Compliance Sheriff® and Sheriff Workflow™.

Deploy: Deploy Compliance Sheriff and HiSoftware Security Sheriff™ to scan and tag content to automatically detect, correct, prevent, and mitigate risk.

4 AUTOMATE CONTENT COMPLIANCE

Integrate with User Activities: In addition to scanning content at rest for violations, Compliance Sheriff also reviews content as it is created to automatically mitigate risk by flagging violations and classifying content based on the pre-defined policy rules, while appropriately notifying stakeholders.

TIPS FOR SUCCESSFUL & CONSISTENT CONTENT COMPLIANCE

- Ensure the content compliance strategy aligns with the organization’s overall strategy and is updated for changes to existing and new policies and laws.
- Make sure the Governance framework is relevant and updated regularly.
- Have key stakeholders review the strategy regularly.
- Implement a solution to continuously audit content, detect violations and enforce compliance policies to maintain data integrity and security, and employee and customer confidence.

5 SECURE CONTENT

Secure Content: With Security Sheriff the system can also restrict access to, encrypt, track, and prevent the publishing of content based on the presence of sensitive and non-compliant information.

Monitor & Evaluate: Workflow can be used to remediate compliance issues and/or task the proper individual(s) in the organization to review and potentially quarantine, remove, classify or re-classify the content. Central workflow also allows policy officers to override approvals and user actions, and make adjustments to classifications.

6 REPORT, REMEDIATE & REFINE

Audit & Report: Confirm compliance with defined policies, report on compliance and security status of sites and measure progress against goals over time, while providing an audit trail for regulators.

Remediate & Refine: Detailed reports that pinpoint the location of problems allow users and developers to remediate issues quickly. Accurate reporting also allows policy managers to modify policy and workflow rules based on user interaction and compliance trends.

PROTECT THE ORGANIZATION

Scan & Audit: Scan content at rest or in motion to detect non-compliant data and violations.

Report: View the compliance status of the site(s) and incidences, measure progress, and pinpoint issues for remediation with detailed reports and dashboards.

Classify: Classify data at the file level based on pre-defined policies or users can manually classify data using pre-defined values.

Restrict: Set file permissions based on metadata. This limits collaboration of non-compliant documents.

Encrypt: Further secure sensitive content by encrypting it immediately so only properly credentialed users will be able to read the content – whether inside or outside of SharePoint.

Prevent: Prevent users from publishing, distributing, or emailing confidential and sensitive documents.

Control: Trigger workflows to alert users to fix issues, get manager approvals, and quarantine documents.

Track & Monitor: Monitor the movement of confidential and sensitive documents, including who views, prints, and emails the documents.

© 2012 HiSoftware Inc.