Balancing Transparency and Privacy: Best Practices to Protect Your Sensitive Data

Dan Wilkens, Esq.
Software Product Analyst
AvePoint, Inc.
Presenter For Today

Dan Wilkens, Esq.
Software Product Analyst
AvePoint, Inc.

Contact Information

@TheDanWilkens

linkedin.com/in/danwilkens

daniel.wilkens@avepoint.com
Today’s Agenda
Agenda

Seeing the Big Picture

AvePoint Compliance Methodology

4 Steps to Compliance Success

Concluding Remarks and Q & A
So where do we begin?
it all starts with one word:

Banana

chalupa? wrong
it all starts with one word: trust
Foster trust with transparency and privacy

**Trust In:**
- Individuals
- Organizations
- Policies
- Procedures
- Process
- Technology
- Transactions
Big data

GET ALL THE INFORMATION YOU CAN, WE'LL THINK OF A USE FOR IT LATER.
Disruptive Technologies

Everyone has a Voice
Social Collaboration

Access from Anywhere
Cloud, On-Prem, Mobile

Everyone is a Contributor
Welcome to the jungle.
Creating and maintaining a compliant collaboration environment is a continuous process

Transparency and Collaboration

People
Policy & Process
Technology

Data Protection and Management

Training
Governance & Oversight
Technical Enforcement
There is a Trade-off

Prolific global access and interaction

Securing sensitive information
“Collaboration with Confidence”

- Transparency
- Collaboration
- Data Protection
- Compliance
So why is this important?
100+ TB of content stolen
Thousands of confidential emails by CEO
Movies leaked to public and cancelled due
to terror threats
Employee PII leaked
Tied to international politics
One multinational company brought to its knees
Let’s start with an example...
Be careful what you ask for...
Lessons to be Learned

• Information must be accessible & available to the people who should have access to it
• Should be protected from the people who should not
• This information can reside on or be surfaced on-premises, in the cloud, in various databases, on mobile devices and across social collaboration and messaging platforms
• This information may need to be stored, archived and preserved for some period of time
• Need to consider the entire content lifecycle here
AvePoint Compliance Methodology
AvePoint Compliance Methodology

**Assessment**
1. Analyze
2. Identify
3. Prioritize

**Design**
4. Diagram
5. Structure

**Optimization**
6. Undertake Migration

**Control**
7. Maintain Control
Step 1: Assess the situation
Compliance Assessment

Develop 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. Compliance Officers and other key stakeholders can use this information to react swiftly to investigate and resolve any potential issue.

Key Activities
- Analyze the Current Environment
- Identify Non-Compliance
- Prioritize the Business Need

Exit Criteria
The assessment phase will result in a baseline report that reviews the “as-is” 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.
Key Activities: Assessment

1. Analyze the Current Environment
   Identify non-compliant data across a broad framework of organizational or regulatory requirements: Privacy, Security, Accessibility, Sensitive Security Information, Brand Management & Site Quality

2. Identify Non-Compliance
   Answer the key "who, what, when, where, and how" questions for content inside your organization to identify key areas of risk

3. Prioritize the Business Need
   Aggregate compliance scan results across one or many environments
   Gain insight by aggregating usage data, activity history, permissions, & content at any level of granularity
check yourself before you wreck yourself
Best Practices: Environment Assessment

Plan First, Act Later
Assessing the scope of your environment may be much harder than it seems

- Microsoft stack of products
- Line of business applications
- Legacy systems and file shares
- File sharing silos
- Mobile devices
Collaboration extends beyond your internal workforce
End-users need to share content outside the firewall as a part of their jobs
• From laptops, tablets, mobile devices
• From SharePoint, Outlook, Office, etc.

Questions to Ask:
• How do your end-users collaborate with people outside your company?
• Who do they collaborate/share content with?
• Do you restrict access to content on mobile devices?
• How do you prevent data leakage?
• How do you exercise control over this?
Detailed Assessment Steps

1. Review Compliance Requirements
2. Set Scope for Initial Test
3. Initial Smoke Test
4. Review Results/Refine Rules with early project owners
5. Initial Baseline Scan
6. Results Analysis and Documentation
7. Results Presentation Meeting
8. Mitigation Recommendations

Initial Meeting
Step 2: Design control processes...
Design

Data from the assessment will be used to develop a comprehensive risk management plan as well as restructure, reclassify, reorganize, and even potentially retire data that will not only improve the compliance posture of the organization, but also will likely lead to improved SharePoint performance.

Key Activities
- Classify and Structure Information
- Determine appropriate permissions and security settings
- Prioritize recommended changes to streamline the future implementation of a restructured compliance framework
- Strictly regulate user-generated content to prevent the creation or uploading of non-compliant, harmful content

Exit Criteria
The Design Phase will deliver a data classification and governance plan with buy in from key stakeholders – that can be implemented and automated through technology as part of the optimization effort. This plan will be a living and constantly evolving plan so that there is a continuous feedback loop of Risk Management improvement and system hardening.
Key Activities: Design

Diagram New Security Boundaries
Determine appropriate permissions & security settings based on the governance and compliance requirements of SharePoint or file-based information

Classify and Structure Information
Utilize highly customizable business rules to classify content as it is uploaded or created with metadata, ensuring sensitive or regulated content can be appropriately tracked and organizations can accurately determine risk levels of their information
Best Practices: Information Review

What information needs to be protected?
Assess your existing policies on content to access security risks
  • 80/20 rule
  • Think about how to separate the wheat from the chaff

Example: Business records vs. non-business records
  • How do you define a record?
  • What policies do you have to comply with?
  • How long do you need to keep it?
  • Who is responsible for it?
  • Restricted vs. public
  • Sensitive vs. who cares
Best Practices: Architecture

Create strong, well-managed containers that correspond to governance policies
- Automate site provisioning -- give end-users a questionnaire to fill out to create the sites they need.
- Can use this method to standardize and increase uniformity
  - IT admin is able to configure policies that regulate how backup, archival, and permission management/recertification is handled. Set content types, classifications, etc.

Provisioning is the tip of the iceberg
Supplant the helpdesk and give them means to send service requests for SharePoint.

Classify data upon upload and associate retention and destruction policies with it
- Use content types to enforce records management principles
- RM is a wide discipline with many ways to envision it
- RM is also a way to manage / protect data
Step 3: Optimize and balance...
Optimization

Implement an information architecture and data monitoring management and classification schema to address compliance and governance requirements for all SharePoint and network content.

Key Activities

- Scan multiple content sources
- Tag content with imbedded or system metadata
- Based on content classification, assign permissions, route to the appropriate location, or block or quarantine to comply with information governance policies
- Support user-driven "assisted" tagging and/or automated tagging

Exit Criteria

The optimization phase will deliver a restructured and compliant environment. Content will be classified and protected to ensure compliance with information governance, security, and architecture policies by blocking, quarantining, securing, or routing content based on its classification and implementing monitored and controlled role based access.
Undertake Optimization of "as is" to "compliant" environment

Based on content classification, block or quarantine non-compliant content; route content to the appropriate location; and apply appropriate security and permissions to ensure compliance with information governance, security and architecture policies.
Step 4: Execute...
Control

Continuous scheduled and real-time scanning, tagging, classification and action will allow the organization to pinpoint risk with a customizable risk calculator and to quickly identify and correct problems.

Key Activities

- Implement scheduled and real-time scanning, tagging, classification, and protection of data.
- Identify inconsistencies between document and system or SharePoint metadata, and synchronize to ensure metadata consistency across platforms.
- Quarantine or remove sensitive or inappropriate content from SharePoint to prevent spillage and other forms of environment contamination.

Exit Criteria

The control phase will allow the organization to maintain a best practice approach for remediation of any identified compliance issues. Prioritize recommended changes to streamline the future implementation of a restructured compliance framework and to maintain a historical view of their compliance status over a period of time to demonstrate statutory compliance and maintain a complete audit trail.
Key Activities: Control

Maintain Control

Easily audit security settings, investigate usage patterns, and monitor sensitive information to assess the effectiveness of the risk management strategy.
Assess

Design

Execute

Optimize
AvePoint Methodology Recap

1. Analyze
2. Identify
3. Prioritize
4. Diagram
5. Structure
6. Migrate
7. Maintain Control

Enterprise Risk
Collaborate with Confidence

By identifying, classifying, and taking action on compliance risks - and presenting this information in easily digestible formats for various stakeholders, organizations can more effectively build and maintain a compliant framework.

Prevent-Proactive policy enforcement and automation to control access, direct content, and prevent content leaks and misuse.

Detect—Quick detection of events, if and when compliance infractions occur

Track—Complete investigations with knowledge of who, what, when, where, why, and how a breach occurs.

Respond and Resolve—Quick corrective action including legal holds, archiving and removing content from unprotected areas, and restructuring access to prevent the likelihood of a future breach.
Our Resources: Learn More AvePoint

Visit www.AvePoint.com/Resources

White Papers
eTutorial Videos

Customer Success Stories