Meeting Compliance Objectives in SharePoint®

This document is intended to aid IT administrators and other stakeholders responsible for managing Microsoft® SharePoint® deployments, in planning and implementing a comprehensive, reliable and efficient compliance strategy appropriate to their organizational needs.

AvePoint

Unleashing the Power of SharePoint™

Table of Contents

Table of Figures

Executive Summary

In recent years, the business and political landscape has seen incredible change with regard to the rules and regulations governing the stewardship of electronically stored and processed information. A flurry of new regulatory and statutory initiatives – prompted by several high profile corporate and government scandals – has made it imperative for organizations to develop and implement robust compliance strategies for their information management systems and overall IT infrastructure. Though today's regulatory and legal landscape is expansive and diverse - with numerous government entities and accrediting agencies contributing to a myriad patchwork of rules and statutes – at the heart of virtually all IT-related regulations is an effort to protect the integrity, confidentiality, and availability of information impacting the stakeholders of a given organization, industry, or constituency.

Microsoft SharePoint has empowered organizations to realize unprecedented levels of productivity and efficiency, but its adoption also presents distinct compliance-related challenges. The very characteristics of the platform that make it such a potent and popular business tool – its ease of use and propensity for 'bottom-up' growth – make the implementation of compliance initiatives both critically important and uniquely challenging.

This document will first briefly review the general principles underlying today's regulatory and legal environment, then analyze how these principles can translate to concrete SharePoint compliance strategies. Though the regulatory framework today's organizations face is dynamic and can vary by both country and industry, we can – for our purposes here – benefit from analyzing the entire regulatory ecosystem through the prism of the five major regulations that govern much of today's business and civic activity.

We will then analyze SharePoint's native capabilities to meet these compliance obligations, reviewing both the out-of-the-box tools and the procedures by which administrators can implement these tools to meet compliance demands. To help elucidate these procedures, we will walk through several compliance-related tasks organizations often face, highlighting both best practices and potential hurdles.

Finally, we will review strategies organizations can adopt to streamline and optimize their compliance initiatives. We will briefly analyze the financial and legal cost/benefit of such strategies, and using our common compliance tasks as examples, describe how organizations might leverage these tools to achieve a more robust, efficient, and manageable compliance strategy.

This document is intended to aid IT administrators and other stakeholders responsible for managing SharePoint deployments, in planning and implementing a comprehensive, reliable, and efficient compliance strategy appropriate to their organizational needs.

Compliance Defined

Compliance has become one of the most pressing and daunting concerns for organizations worldwide. Regardless of size and activity, companies are likely affected by some combination of regulatory and internal compliance obligations, composed of a mix of international, federal, local, and industry-specific regulations, and internal 'best practice' protocols.

The term "compliance" is a word that has undergone an evolution of meaning as the IT industry has itself evolved. People and procedures can comply with all sorts of things, but what exactly do we mean by compliance when we discuss IT infrastructure management? So, before we proceed with a discussion about compliance, let's broadly define the term for our purposes here, then define a few additional, more concise terms that might help us focus our discussion.

Compliance is the act of conforming to a specification or policy, standard or law. Simply put, it means "following the rules." For today's business and civic organizations, the term is generally used in reference to all the various regulations, statutes, internal procedures, and best practices they are compelled to follow when conducting their operations.

This discussion will focus specifically on strategies for achieving effective compliance with regard to the operation of SharePoint, Microsoft's popular collaboration and portal platform.[1] This topic falls within the broader theme of IT compliance, which we can define as: the initiatives, technical controls, and procedural controls established and executed by or for an organization to ensure its IT infrastructure, the users of that infrastructure, and the information that it supports, operate under applicable laws, standards, and policies. Based on this definition, we can see that no software can claim that it "guarantees compliance" with a given regulation. Rather, a software vendor can state that its product delivers all of the technical controls required to achieve such compliance. It is the responsibility of the complying organization to correctly and diligently implement these technical controls – in conjunction with appropriate procedural controls – to satisfy a particular obligation. This holds true for all SharePoint Products and Technologies, and all solutions that support the platform.

Organizations face increasing pressure to comply with government regulations and best practice prescriptions for handling sensitive information stewarded via IT infrastructure. These rules are designed to protect against a wide range of risks that span different industries, and have received heightened attention in recent years.

- A surge in identity theft and fraud has prompted stricter regulation with regard to the handling of personal identifiable information (PII) that is electronically-stored and processed.

---

[1] For purposes of this document, we will limit our discussion to the compliance-related capabilities of Microsoft Office SharePoint Server 2007 (MOSS).

- Recent invasions of the privacy of individuals have prompted regulations for handling electronically-stored and processed personal health information (ePHI).

- High-profile corporate scandals have resulted in an increase in the number and breadth of compliance regulations intended to protect organizational stakeholders, and improve the visibility, integrity, and accountability of financial reporting.

- Risks related to food and pharmaceutical production and consumption have inspired elevated regulation for all suppliers of such products.

- The exponential growth in both the scale and scope of information housed and stewarded electronically by organizations across all sectors has prompted an increased effort to develop more robust internal compliance protocols.

The consequences of not developing and maintaining an adequate compliance strategy – financial penalties, exposure to punitive litigation, and loss of reputation, among others – have made compliance a primary concern for organizations throughout the civic and business community. Increasingly, organizations are not simply viewing compliance initiatives as a cost of doing business, but are also embracing it as an opportunity to make business processes more efficient and profitable. As a result, even organizations that are not subject to certain compliance regulations often adopt certain prescriptions in order to capture additional business value and burnish their reputations.

Key Regulations Affecting IT Compliance

It is impossible to comprehensively analyze all the statutes and guidelines that regulate or recommend IT-related protocols. As we shall see, however, the objectives established by the overwhelming majority of them are largely similar in both scope and approach. Therefore, by reviewing the components of five major regulations (actually, four regulations and one guideline), we can distill the central objectives and strategies prescribed by the great majority of IT compliance initiatives.[2] For expediency, in the main body of our discussion we will simply summarize how each regulation/protocol directly addresses IT compliance, and outline the prescriptions it directs. For reference, in the endnotes of this document we provide the exact language of each regulation, as it pertains to IT compliance.[3]

- **Sarbanes-Oxley Act of 2002 (SOX)**
  The Sarbanes-Oxley Act was enacted in the United States in response to numerous corporate scandals involving inadequate and/or fraudulent accounting and auditing procedures. From an IT compliance perspective, the most relevant section of the Act is Section 404, which requires publicly traded companies to yearly assess the effectiveness of

---

[2] Indeed, if an organization is subject to an IT compliance regulation or guideline, it is likely to be one of these five, or a regulation/protocol derived from the prescriptions detailed in one of them.

[3] Please note: This document is not a comprehensive resource on IT compliance, but rather a brief review of compliance objectives and selected approaches. To receive guidance concerning specific compliance planning, consult your organization's legal counsel or auditor.

the internal controls in place to ensure accurate financial reporting. SOX also requires that all publicly-traded companies engage an independent auditor who must attest to, and report on, the validity of the company's assessments. This regulation is enforced by the U.S. Securities and Exchange Commission.[i]

- **Health Insurance Portability and Accountability Act of 1999 (HIPAA)**
  The Health Insurance Portability and Accountability Act was enacted to streamline dispensation of healthcare in the United States, and ensure adequate management of consumers' personal health information (PHI) and electronic personal health information (ePHI). The privacy and security rules for this act must be followed by not only companies within the U.S. healthcare industry, but also those that engage in certain related activities, such as managing employee group health plans or providing services to companies that this regulation directly affects. This regulation is enforced by the U.S. Health and Human Services Department.[ii]

- **European Union Data Protection Directive – 95/46/EC (EUDPD)**
  The EUDPD enforces baseline requirements for data privacy which all member countries must achieve via national regulation. Created to protect the privacy of citizens of EU countries, the Directive has a profound influence on international regulations because of the limitations it places on sharing personal information about EU citizens outside of the EU in areas deemed to have less than adequate data security standards. Hence, EUDPD – and the various regulations enacted pursuant to it – affect companies that do business in the EU or handle the data of EU citizens. Various regulatory agencies of EU member states are tasked with enforcing the national regulations based upon the Directive.[iii]

- **Title 21 CFR Part 11 – Federal Food, Drug and Cosmetic Act**
  Title 21 CFR Part 11 deals with the U.S. Food and Drug Administration's guidelines on records and electronic signatures in the United States. Part 11 requires drug makers, medical device manufacturers, biotech companies, biologics developers, and other FDA-regulated industries to implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing electronic data that are required to be maintained by the FDA's predicate rules or used to demonstrate compliance to a predicate rule.[iv]

- **ISO/IEC 27002 Code of Practice for Information Security Management**
  The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provide standards and best practice recommendations for a wide array of manufacturing and management processes. Standard 27002 (formerly ISO/IEC 17799:2005) provides best practice recommendations on information

Regulations generally do not prescribe particular tactics or tools for meeting their objectives, but rather articulate approaches and strategies that are appropriate.

security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS). Though this standard takes a very broad approach to information security for electronic files and communications, and is not a regulation per se, it is regularly cited by regulations as a prescribed guideline. Hence, ISO/IEC 27002 serves as a touchstone protocol for organizations wishing to mitigate exposure to risk of litigation, and provide appropriate means to respond to various legal requests for electronic information.[v]

Though each regulation differs, these five serve as a representative sample of compliance initiatives currently in force that directly address IT processes and operations. As each regulation's language reveals (presented in the endnotes corresponding to each of the summaries above), regulations generally do not prescribe particular tactics for meeting their objectives, but rather articulate approaches and strategies that are appropriate. Generally – because regulatory agencies seek to be technology neutral – the prescriptions themselves are broad, and do not define discrete tools or methods.

Common Objectives of IT Compliance

Though these regulations/protocols vary in the industries they oversee and the jurisdictions in which they are exercised – we can distill from them a common set of objectives:

Common Objectives of IT Compliance	
Confidentiality	Confidential, personal, and sensitive information cannot be exposed to unauthorized organizations or individuals.
Integrity	Data cannot be modified by unauthorized organizations or individuals, and both completeness and accuracy must be insured.
Availability	Information must be available to the right people at the right time to support timely and accurate financial reporting and to fulfill demands for information by regulators, investigators, and court subpoenas.

Figure 1: Common Objectives of IT Compliance

For compliance purposes, just as important as the objectives themselves is the ability to meet both these objectives efficiently and evidence having met them. Therefore, the following two objectives are requisite ancillary goals of any robust compliance strategy:

✓ **Procedural Rigor:** An organization must seek to meet it compliance objectives via systems and practices that make it as automatic and unobtrusive as possible. This minimizes the risk of human oversight and error, and makes the task of confirming compliance as efficient as possible for the regulatory agency involved.

✓ **Auditing and Logging:** Auditing and logging records how individuals access and use regulated resources. Systems that process sensitive data

must securely log, maintain, and provide critical event information to ensure a clear audit trail for all regulated resources.

Audit trails and logging are a critical component of IT compliance for organizations attempting to both (1) meet regulatory obligations, and (2) mitigate exposure to legal risk.

With regard to regulatory obligations, auditing facilitates integrity controls and enables the delivery of required documentation to regulators. Auditing provides regulators with the records they need to confirm that an organization is actively ensuring the confidentiality, integrity, and availability of regulated data. Additionally, in cases when technology is not able to fully ensure data integrity by stopping an authorized user from accessing or modifying information, an audit trail empowers the organization to understand the impact of the incident and take corrective action(s).

In preventing legal exposure (from both regulatory agencies and 3rd parties), robust auditing is crucial in determining the scope of disclosures of confidential information. Being able to establish what information was accessed (and by whom) allows an organization to inform just the people whose information was compromised, sometimes greatly reducing the fines and other costs associated with the incident.

Meeting Compliance Obligations Through Effective Controls

Meeting these objectives requires a variety of measures, and each organization must develop strategies particular to its industry, regulatory obligations, business processes, and legal requirements. The measures used to meet compliance obligations are defined by the *controls* they implement. For our purposes, a control can be defined as "a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system."

Controls can be broadly classified into two categories: Business Controls and IT Controls. Though both types of controls are meant to protect and optimize business operations, they can be thus broken down based upon how they are implemented. Business Controls regulate and guide the business processes of the organization. IT Controls regulate and guide the operations of IT infrastructure within the organization, including all the systems and processes within it. A comprehensive compliance strategy requires both appropriate Business Controls and IT Controls. Because the subject of our discussion is the satisfaction of compliance obligations with regard to SharePoint, we will primarily focus on the IT Controls available for such a task.[4]

---

[4] **IT Control Classification -** IT controls can be classified as either *manual* or *automated*. Manual controls require a person to enforce the control, whereas automated controls are enforced by the IT system itself.   Between the two, automated controls are generally more desirable, because after appropriate testing, these controls can be relied upon to operate consistently – not exposing the organization to the risk of human error or oversight.   IT controls can be further classified as either *preventive or detective*. Preventive controls prevent unwanted events from occurring. Detective controls, on the other hand, detect events and notify a person or system to respond to them. Preventive controls are superior to detective controls in that they thwart non-compliant activities before they occur.   A comprehensive IT compliance program includes some combination of controls from each of these various classes.

With our compliance objectives identified, we can now review the challenges posed to organizations running SharePoint. We will then review the features, or IT Controls, SharePoint provides 'out-of-the-box' to assist in compliance satisfaction, and to identify where more robust solutions might be required. To put this discussion in a real-world context, we'll use the example of an imaginary organization – ACME Inc. – and review how it can attempt to meet its compliance objectives.

SharePoint – A Powerful Platform and Potent Compliance Challenge

SharePoint is the fastest growing product in Microsoft history[5] for a reason. Organizations have recognized the platform's unmatched ability to serve as a centralized document repository, online collaboration workspace, intranet, extranet, and portal service. As adoption of SharePoint continues to accelerate globally – spreading into every industry vertical and market – growing numbers of organizations are confronting the formidable challenge of governing and monitoring the platform's infrastructure and activity, and ensuring the deployment remains compliant with applicable regulations and internal protocols.

SharePoint is unique in that the many virtues of the platform also serve as the fundamental reasons why it is challenging to efficiently meet compliance objectives. SharePoint is, by design, meant to be a 'grass roots' tool. By 'grass roots,' we mean it is a centralized platform whose end-users are the primary contributors of content and developers of processes. This allows for exceptional usability and productivity, but can make the governance and management of the platform difficult. Since both the topology and the content of SharePoint is usually quite dynamic and ever-changing, discovering and controlling what is on the platform and how it is organized can be difficult. Because the end-user base is constantly changing, discovering and managing securities and permissions can be labor intensive and tedious. And finally, as a collaboration platform and asset repository for unstructured data, the *metadata* (or "data about the data" – such as last modified date, created by, creation date, etc.) of SharePoint content becomes as critical as the data itself. Given the relative autonomy end-users can exercise within the platform when permissions and securities are not effectively managed, protecting this vital information can prove difficult.

Achieving Compliance with Native Tools

Let's now review how each of the compliance objectives we outlined in the previous section – confidentiality, integrity, and availability of information - can be achieved with respect to SharePoint. For each of these objectives, we must also review how

---

[5] In March 2008, Bill Gates reported that Microsoft expects SharePoint to earn USD 1bn in revenue by year's end, setting a record for progress to that level of revenue among the firm's products.

suitable procedural rigor and auditing can be delivered. With this understanding, we will be able to identify if, and where, there are areas where more robust functionality might be needed.

Maintaining the Confidentiality and Integrity of Information

Preventing the exposure of sensitive data to unauthorized users, and ensuring its complete access to those so authorized, are formidable challenges in SharePoint. To do this with procedural rigor and appropriate auditing can prove nothing short of daunting. In Figure 2 below, we review the key requirements an organization running SharePoint must satisfy with regard to these objectives:

Requirements for Maintaining the Confidentiality and Integrity of Information	
Account Stewardship	✓ End users have access to only those SharePoint elements for which they are authorized ✓ End users have modification rights to only those SharePoint elements for which they are authorized ✓ End users are prevented from introducing non-compliant content to the SharePoint deployment
Auditing	✓ Recording of all events associated with maintaining the integrity of information stored on the platform ✓ Recording of all events associated with maintaining the confidentiality of information stored on the platform ✓ Generate timely and accurate records of all SharePoint events associated with maintaining the integrity and confidentiality of information, from the object, user, and action perspective
Procedural Rigor	✓ Efficiently maintain and manage permissions associated to users and elements without excessive burden being placed upon IT staff and management ✓ Satisfy reporting requests with a level of precision that empowers the organization to react swiftly to regulatory/legal requests and non-compliance events ✓ Satisfy audit storage requirements in a manner that does not burden storage resources or reduce platform performance

Figure 2: Requirements for Maintaining the Confidentiality and Integrity of Information

To highlight these requirements, and to review how their satisfaction can be attempted via SharePoint's native toolset, let's use a real-world example.

Acme Inc., a pharmaceutical company, has a dual-farm SharePoint deployment with the following attributes:

- 11,000 end-users. This end-user base is constantly changing, as approximately 50 new employees join the company and 50 leave weekly.
- 10 web applications

AvePoint

- 50 site collections
- 500 sites, one for each of the company's discrete project teams. Access and modification rights for each site must be given to a dynamic, constantly changing set of end-users who are either part of each site's associated business unit or project group. The composition of these groups is constantly changing according to business needs.
- 100 of ACME's 500 sites contain information that the company is – by regulation – required to maintain a 7 year audit trail that captures all access, modification, and deletion events. Two such sites reside in each of the company's 50 site collections.

Because of ACME's scope of business, it is subject to the jurisdiction of *Title 21 CFR Part 11* of the *Federal Food, Drug and Cosmetic Act*, and its own voluntary internal best practices as prescribed by IS/IEC 27002:2005. First let's identify what ACME has to do to meet information confidentiality and integrity objectives:

Compliance Objectives of ACME Inc. (Information Confidentiality and Integrity)	
Objective #1: *User and Content Management*	✓ All users must be able to only access/modify content for which they have authority. ✓ All users must be prohibited from uploading content considered non-compliant. ✓ As new end-users are introduced to the system, they must be given appropriate rights. When employees are terminated, they must be stripped of rights in a timely manner. ✓ All this must be done without excessively burdening IT staff and resources.
Objective #2: *Auditing User and Content Management*	✓ Audit the access and modification histories of the company's 100 "regulated" sites, two of which reside in each site collection. ✓ Reports based upon this audit data must be generated in a manner that does not excessively burden IT staff and management
Objective #3: *Storing Audit Data*	✓ Audit data must be stored for 7 years, and this storage requirement must not excessively burden system resources or performance.

<p style="text-align:center">Figure 3: Confidentiality and Integrity Objectives of ACME Inc.</p>

Let's see how well ACME could attempt to meet these objectives using SharePoint's native functionality.

Objective #1:   User and Content Management

Natively, SharePoint provides the functionality to discover and configure the permissions of users and elements. However, it is limited in its ability to do so in an efficient manner that does not tax IT resources or expose the organization to excessive risk of human-error. This is because <u>SharePoint does not provide a unified interface through which to discover or manage securities and permissions throughout the deployment</u>. All securities configurations in SharePoint are controlled at the site collection level, (via the Site Collection's Central Administration page), the site level (via the Site Settings page), and the object level (via the object's properties interface). Therefore, reliance solely upon SharePoint means that:

✖ **To discover the permissions a particular user or group has throughout the deployment, an administrator would need to access every site collection, site, and object-level settings interface. There is no way to easily ascertain what a user or group has authority to access/modify deployment-wide.**

✖ **To execute securities changes to a particular user or group, an administrator must access the settings interface of each particular SharePoint element or object for which that user has explicit permissions. There is no way to modify in-bulk the permissions of a particular user or group throughout the deployment.**

✖ **An administrator is unable to set, break, or prescribe exclusion rules to inheritance-based permissions for an end-user or group above the Site Collection level.**

SharePoint has no ability to scan content prior to its upload to the platform, to verify that it is business-appropriate, of the authorized format, or complaint. Therefore:

✖ **An administrator is unable to prevent upload of content considered non-compliant or unauthorized by the organization.**

Given ACME's large and dynamically changing user-base – with 50 new and 50 expelled users weekly, and numerous working groups whose composition is constantly changing – a team of administrators would need to manually discover and modify, and report upon the securities regime of the company's deployment. Because SharePoint does not provide a single interface to manage securities, or the means to discover securities by discrete user, or object, reliance upon SharePoint:

✖ **Forces administrators to dedicate excessive time manually discovering and managing securities of deployment elements and users.**

✖ **Exposes ACME to elevated risk of human-error and oversight.**

Objective #2: **Auditing User and Content Management**

Now let's review SharePoint's auditing and reporting capabilities. <u>SharePoint can perform auditing only at the site collection level</u>, via the *Configure Audit Settings* interface on the Central Administration site. For documents, items, lists, libraries, and sites within the chosen site collection, SharePoint auditing can track:

SharePoint's Native Auditing Ability (per site collection)	
For Documents and Items	• Opening or downloading of documents, viewing items in lists, or viewing item properties • Modification • Checking-out or checking-in • Moving or copying to another location in the site collection • Deletion
For Lists, Libraries and Sites	• Editing content types and columns • Searching site content • Editing users and permissions

Figure 4: SharePoint's Native Auditing Ability (per site collection)

Now that we know what SharePoint can audit, we can identify where it falls short. Figure 5 lists the auditing limitations of SharePoint.

Limitations of SharePoint's Native Auditing Ability
✖ Cannot audit the activities of a particular user or group. **If an organization was required to track the activity of a given end user, they would need to enable auditing on every site collection throughout the deployment, then distill the user's activity from the copious audit data thus created.**
✖ Cannot audit the deletion of sites. **The accidental or malicious deletion of a site cannot be recorded.**
✖ Cannot enable auditing at any level other than the site collection. **Though organizations may select which actions are audited from those listed in Figure 4, doing so means that all such activities throughout the site collection are audited. There is no ability to enable auditing granularly, at the site, library, list, or object-level.**
✖ Cannot store audit data anywhere other than in the deployment's associated SQL Server database. **Native SharePoint audit data must be stored on SharePoint's database. In ACME's case, the requirement to maintain a 7-year audit history demands significant storage space. Considering SharePoint's inability to audit below the site collection level and the relative expense of SQL storage space, ACME's audit storage requirements would be cost prohibitive, and negatively impact the performance of the platform.**

Figure 5: Limitations of SharePoint's Native Auditing Ability

Now let's review SharePoint's native ability to generate reports based upon this audit data. At the site collection level, SharePoint provides a number of reports based upon audit data. The reports are listed in Figure 6, below.

SharePoint's Native Audit Reporting (per site collection)	
Content modifications	Report displays all events that modified content in the site collection
Content type and list modifications	Report displays all events that modified content types and lists on the site collection
Content viewing	Report displays all events where a user viewed content in the site collection
Deletion	Report displays all events that caused content in this site

AvePoint

	collection to be deleted or restored from the Recycle Bin
Expiration and Disposition	Report displays all events related to the expiration and disposition of content
Policy Modifications	Report displays all events related to the creation and use of information management policies
Security Settings	Report displays all events that change the security configuration of SharePoint
Auditing	Report displays all events that change the auditing settings of SharePoint

Figure 6: SharePoint's Native Audit Reporting (per site collection)

With this, we can assess the limits of SharePoint's native audit reporting capabilities, in terms of both their breadth and flexibility. These limitations are listed in Figure 7, below:

Limitations of SharePoint's Native Audit Reporting	
All reports are "action-centric"	Because all auditing is action-centric (e.g. "Report all modification events"), in order to generate a report based on a particular user or discrete object, an administrator must either (1) script a query directly to the SQL database, or (2) script a query through the SharePoint object model.
Reports are not time-sensitive	It is impossible to generate a report based on time parameters. All reports generated will include all audit data provided since the auditing was enabled.
All reports are at the site collection-level	Reports cannot be generated for any scope other than the site collection level. For deployment-wide audit reports, or those delivering results for any other level of the SharePoint deployment hierarchy, administrators must either (1) generate the appropriate report within every site collection in the deployment, then distill the required information, or (2) programmatically script a SQL or SharePoint object-model query that performs the operation.

Figure 7: Limitations of SharePoint's Native Audit Reporting

Objective #3:   Storing Audit Data

As we've discussed, all audit data derived from SharePoint's native audits must be stored directly in the deployment's associated SQL server database, and must remain there in order to deliver reports. As we have also discussed, SharePoint can only enable auditing at the site collection level. These two aspects of SharePoint's native auditing functionality combine to limit ACME's ability to meet Objective 3 in the following ways:

> ✖ **Though ACME required auditing for only one site in each of its site collections, utilizing SharePoint's functionality, they would have to**

AvePoint

enable auditing for all of its site collections to capture audit data for the one "regulated" site in each of them. This necessitates a large amount of unnecessary audit data, and – given the high relative cost of SQL storage – places an excessive cost-burden on the company.

✖ **Because audit data must remain in the SQL database, over time, the deployment's database resources will become laden with audit data. Not only is the audit data unnecessarily large in scope, but it cannot be removed from the deployment database without loss of reporting capability.**

As our ACME example has revealed, reliance solely upon SharePoint's native toolset limits ACME's ability to ensure the confidentiality and integrity of its data to compile and produce an appropriate audit record, and to do so with procedural rigor. Now, let's discuss how an organization might approach the task of meeting the final compliance objective we identified: maintaining the availability of information.

Maintaining the Availability of Information

Maintaining the availability of information stored in SharePoint – and ensuring it is done so with procedural rigor and with appropriate auditing – involves several different requirements. To assist our analyses, we can break these requirements down into the following categories:

Requirements for Maintaining Availability of Information	
Platform Reliability	✓ An organization's SharePoint deployment must be appropriately stable and reliable to ensure that stakeholders can access it when needed ✓ Robust disaster recovery and/or high availability solutions must be implemented[6]
Active Content Protection	✓ An organization's live (or "active") SharePoint content must be protected in a manner that mitigates risk of irretrievable loss ✓ Appropriate backup and recovery strategies must be developed and implemented in accordance with business-appropriate Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO)[7]
Efficient Access to Historical Content	✓ An organization must not only have access to SharePoint's active data, but, in many circumstances, to every data iteration that has been stewarded or housed in the deployment throughout the audit period (for regulatory compliance) or potential statute of limitations (for litigation events)

Figure 8: Requirements for Maintaining Availability of Information

---

[6] Though this document will briefly review strategies and solutions for optimizing SharePoint platform protection, for a more detailed review and analyses of this subject, AvePoint has prepared several white papers and case studies. Please see the reference guide at the end of this document for more information.

[7] Though this document will briefly review strategies and solutions for optimizing protection of active SharePoint content, for a more detailed review and analyses of this subject, AvePoint has prepared several white papers and case studies. Please see the reference guide at the end of this document for more information.

AvePoint

Satisfying auditing and logging objectives with regard to maintaining information availability demands that organizations have specific capabilities. These can be broken down into the following three categories:

Requirements for Auditing the Maintenance of Information Availability	
Platform Availability Reporting	✓ Organizations must be able to record and report upon all events associated with maintaining the availability of the platform, including server configurations, farm-level settings, and web application-level settings. All information related to such changes, including what was changed, when it was changed, and who changed it, must be recorded.
Active Content Reporting	✓ Organizations must be able to record and report upon all events associated with active data protection, including backup and recovery processes, site deletions, and object deletions. All information related to such events, including success/failure histories, and change statistics, must be recorded.
Historical Content Reporting	✓ Organizations must be able to record and report upon historic iterations of SharePoint data. (i.e. they must be able to access data as it appeared in the deployment in the past, and be able to report upon the events that have altered this data. These events include how it was modified/accessed/deleted, by whom, and when.)

Figure 9: Requirements for Auditing the Maintenance of Information Availability

To ensure procedural rigor in this initiative, organizations must ensure the following capabilities with regard to maintaining information availability:

Requirements for Procedural Rigor with Regard to Information Availability	
Efficient platform maintenance	✓ Efficiently apply platform-level configuration changes, policy settings, and perform farm-level maintenance without excessive burden being placed upon IT staff, management, and members of the end-user base.
Efficient Active Content Protection	✓ Efficiently enact data protection strategies without excessive burden being placed upon IT staff.
Efficient Audit Data Storage	✓ Satisfy audit storage requirements for all information availability events (platform, active data, and historical data) in a manner that does not burden storage resources or reduce platform performance.
Deft, Precise, and Timely Audit Report Preparation	✓ Satisfy audit reporting requests with a level of speed and precision that allows management to react to regulatory, legal and internal-review requests.

Figure 10: Requirements for Procedural Rigor with Regard to Information Availability

Based on the requirements laid out in Figures 8, 9, and 10, we can articulate three objectives an organization must meet with regard to the availability of information:

Compliance Objectives of ACME Inc. (Information Availability)	
Objective #1: *Platform Availability Management*	✓ Efficiently maintain and document platform reliability, via appropriate platform protection and disaster recovery strategies. ✓ Limit platform configuration access to only those so authorized ✓ Enable auditing on its platform protection and configuration activities, and generate reports based on this audit data in an efficient manner
Objective #2: *Active Content Availability Management*	✓ Efficiently maintain and document Active Content Protection strategies. ✓ Enable auditing on these activities, and generate reports based on this audit data in an efficient manner. ✓ Search and discover all responsive active content efficiently, and export search results in a format appropriate to regulatory or legal requests.
Objective #3: *Historical Content Availability Management*	✓ Enable access to historical information when required, in a manner that does not burden system resources ✓ Efficiently deliver reports upon this information for regulatory or legal review upon request

Figure 11: Availability Objectives of ACME Inc.

Let's review how these objectives can be met using SharePoint's native toolset. To help our discussion, let's again use our real-world example, ACME Inc.

Objective #1:   Platform Availability Management

Natively, SharePoint provides limited platform-level protection capabilities. Nominally, an administrator would attempt to recover the platform in one of two ways: via a SQL database restore or utilizing SharePoint's native restore functionality.

During a SQL database recovery, an administrator must first restore the various SharePoint databases (Administration, Configuration, Content, Search, and Index) then independently restore the Front-end Web server configurations and customizations. This is an inefficient process because:

> ✖ **Logistically, the backing up of all the SharePoint servers (Administration, Configuration, Content, Search, and Index) at the exact same time is virtually impossible.   As a result, administrators must attempt to reconstruct the deployment using server backups in different states of configuration and content.**

The other choice organizations have to perform native platform protection – utilization of SharePoint's Central Administration backup utility - is at best a "bare bones" option for several reasons:

> ✖ **Central Administration backups do not protect several key services and databases, including all WFE customizations and**

AvePoint

configurations. A separate backup utility must be leveraged to protect these vital SharePoint platform components.

✖ **Central Administration backups cannot be scheduled and are very resource intensive. As a result, they must be manually performed during non-production hours - likely leading to productivity loss.**

Another important consideration for platform management centers on the permissions required to perform management tasks and how these permissions are delegated. Limiting authority to platform configuration is a labor-intensive process using SharePoint's native functionality. During the deployment and maintenance of a SharePoint platform, there are generally anywhere from three to 10 accounts with some ability to effect platform configuration changes. Because of the large number of administrator accounts and roles (each with their own particular permissions), and SharePoint's inability to manage these permissions efficiently, it is difficult for an organization to delegate to the designated staff-member the discrete permissions required for the platform recovery without giving unlimited rights to the platform.

✖ **If a platform recovery is required, it is impossible to provide the person tasked with re-instating the platform with the granular authority he/she needs to execute the task without providing him/her the "keys to the kingdom" (i.e. providing unlimited access to the platform and all of its configurations and content).**

And finally, reliance on independent SQL database backups and WFE backups to restore the SharePoint platform proffers difficulties in documenting/auditing the process. Though SQL produces its own logs documenting backup events, these logs will not reflect any backups made of WFE customizations or configurations. Such auditing must be enabled via the platform by which WFE backups are being performed (e.g. File System). Hence, when using SharePoint's native tools:

✖ **There is no way to enable a single audit of platform-level backup procedures. Distilling such a comprehensive report from the various SQL logs and WFE backup logs (if these logs even exist) would prove a burdensome and time-consuming process.**

Objective #2:   Active Content Availability Management

Natively, SharePoint offers only limited tools for protecting and searching the active content residing in SharePoint. For protecting the active content, SharePoint provides *Versioning* and the *Recycle Bin*. For searching the active content, it provides *SharePoint Search.* Let's discuss the capabilities of each:

SharePoint's Recycle Bin provides two levels of protection. The user level Recycle Bin provides end users the ability to restore deleted documents to the environment directly. The site collection level Recycle Bin allows designated administrators to restore content that was deleted from the user Recycle Bin. Neither Recycle Bin, however, adequately protects the organization from risk of data loss for several reasons:

AvePoint

✖ **Recycle Bin does not prevent content loss due to corruption. If discrete data is corrupted, the Recycle Bin would only restore the corrupted data.**

✖ **Recycle Bin cannot restore deleted sites.**

✖ **Recycle Bin does not allow the viewing of content prior to restoration.**

✖ **Recycle Bin has default time and size quotas that regulate its automatic pruning. Administrators can disengage these quotas, but doing so would cause the Recycle Bin's content to grow to a volume that could negatively affect platform performance.**

✖ **Recycle Bin does not protect the organization from active content loss due to catastrophic platform failure.**

Enabling Versioning within SharePoint provides an organization with the ability to restore previous versions of a document. Versioning can be enabled to maintain any number of previous versions of a given content item. Versioned content, however, is stored directly on the platform's associated SQL database, so maintaining appropriate versions puts an excessive burden on system resources that can negatively affect system performance. This burden is elevated due to the fact that each retained version is a complete and whole version of the object.

✖ **Versioning on SharePoint requires that all previous versions of an object remain in SharePoint's database, creating a trade-off between (1) maintaining an adequate object history, and (2) system performance and storage space.**

SharePoint Search delivers some functionality to search active content in response to regulatory or legal requests. There are limits to its capabilities, however. Generating exportable reports based on searched materials is not possible via SharePoint Search. Additionally, SharePoint does not let administrators schedule searches. These two critical shortcomings combine to make SharePoint Search an ineffective tool for performing tasks such as eDiscovery, where timely, metadata rich reports are requisite.

✖ **SharePoint Search does not produce exportable reports based on search results. Such functionality is critical when preparing materials responsive to legal and regulatory requests.**

✖ **SharePoint Search does not allow for scheduled searches.**

Objective #3: **Historical Content Availability Management**

Delivering access to historical data leveraging SharePoint's native functionality requires the use of the platform's Records Center. Using Records Center, administrators can archive data, however this process is a complex and limited one for a number of reasons:

AvePoint

- ✖ **A separate SharePoint Records Center must be established for each farm within the deployment. As a result, there is no way to deliver or manage deployment-wide archive data via a single interface.**

- ✖ **The process of delivering content to Records Center can be done manually, or via workflows. Manual delivery demands that organizations rely on its users to diligently archive needed material, exposing the organization to elevated risk of human error/oversight. Workflows, on the other hand, can be established to operate manually or via automated protocols. Designing and maintaining automated workflows for all of an organization's various archiving requirements is a long and tedious process. Managing manual workflows again exposes the organization to risk of human error and/or oversight.**

- ✖ **All Records Center data is maintained within SharePoint – in the associated SQL database. As a result, maintaining extensive archive data can prove an excessive burden on the platform's performance, and negatively affect system performance. Additionally, if the platform becomes unavailable, this archive data is also unavailable.**

- ✖ **Records Center can provide a limited number of reports based upon the data stored within it. However, it is not possible to search these results in accordance with many regulatory and/or legal requests, such as by metadata, user, keyword, or via random sampling.**

Conclusions With Regard to SharePoint's Native Tools

As our discussion has revealed, reliance solely upon SharePoint's native toolset limits an organization's ability to ensure the availability of its platform, as well as its active and historical data. It also limits the company's ability to compile and produce an appropriate audit record of availability, and do so with procedural rigor.

Based on our established compliance objectives (information confidentiality, integrity, and availability, applied with procedural rigor and evidenced via appropriate auditing/logging), it is clear that SharePoint's native toolset does not provide the suitable functionality.

Let's now review solutions available to meet our compliance objectives in a more comprehensive and efficient manner.

AvePoint

Toward More Effective Compliance

In the previous section we used the example of the ACME company to analyze SharePoint's native capabilities to meet the primary objectives of IT compliance. During this process, we identified key areas where SharePoint could not provide the functionality required to meet these objectives in an efficient or comprehensive manner.

Let's review again these compliance objectives, and discuss the many ways one solution – the **DocAve Governance Suite** – can better help organizations meet their compliance objectives.

DocAve® – The Industry's Most Comprehensive Infrastructure Management Solution for SharePoint

The DocAve Software Platform is a full-spectrum infrastructure management software solution for Microsoft SharePoint. With a flexible, fully-distributed modular architecture anchored by a unified, browser-based user interface, DocAve sets the standard for truly scalable, enterprise-strength SharePoint management and protection. DocAve offers eleven modules, each piloted via a single interface but deployable independently – so organizations can craft a solution array to fit their exact needs.

Achieving Compliance Objectives with DocAve

The **DocAve Governance Suite** delivers all the tools organizations need to create and enforce a culture of compliance within their SharePoint deployment. Comprised of seven powerful DocAve modules, the *Governance Suite* is a comprehensive and flexible toolset designed to help organizations prepare and satisfy even the most rigorous legal and regulatory requests. Though the entire DocAve platform is piloted via a single interface, each module is independently deployable, so organizations can create the customized, cost-effective solution they require.

AvePoint

DocAve Governance Suite

DocAve SharePoint Administrator
- Delivers universal control over an entire SharePoint deployment from a single interface
- Easily search, manage, replicate and report configurations and securities of objects and users – granularly or in bulk
- Perform security trimming to delegate management tasks, and maintain efficient permissions regimes with automated account cleaning, cloning and transfer

DocAve Vault
- Archives all SharePoint content in immutable form, with customizable retention policies
- Retains all historical data with full audit history, and stores data securely off of SharePoint with policy based pruning, compression, and encryption
- Delivers fully customizable reports into multiple formats based on any metadata criteria

DocAve Backup and Recovery
- Provides intelligent, item through platform level protection of all SharePoint content
- Protects all platform configurations for fast and efficient recovery of deployment following platform failure events
- Pioneering Business Criticality Matrix automates the backup plan building process for total optimization of storage and system resources

DocAve Auditor
- Records all SharePoint event from the action, object, and user perspective
- Enables full fidelity auditing and reporting of all SharePoint events at any level in the SharePoint hierarchy, from the site collection down to the individual item
- Stores audit data securely off of SharePoint, with automated pruning, compression, and encryption

DocAve High Availability
- Provides a one-switch disaster recovery and platform failure solution via a warm, standby environment
- Maintains a fully synchronized standby environment, accessible via a simply DNS 'switch'
- Ensures zero downtime in the event of disaster or production platform architecture-loss

DocAve eDiscovery
- Scans all active and archived SharePoint content for instances of key word, phrase, metadata tag, or customized criteria
- Delivers fully customizable reports of discovery results in multiple formats
- Allows for scheduled scans of active and archive data to enable tracking of trends, so organizations can make informed decisions regarding platform policies

DocAve Content Shield
- Scans all data prior to upload to prevent upload of non-compliant content
- Provides customizable "black lists" to prevent unauthorized content on SharePoint based on key words, phrases, metadata tags, and file type
- Delivers administrative notifications and quarantines suspect materials to proactively satisfy compliance obligations

Earlier in our discussion, we identified both our compliance objectives and how SharePoint's native tools fall short. Now let's analyze how these objectives can be achieved using DocAve.

Maintaining the Confidentiality and Integrity of Information

Returning to our example company, we identified three objectives ACME Inc. needed to meet in order to satisfy its obligations with regard to confidentiality and integrity of data information stored in SharePoint. Let's break down each of these objectives, and discuss how DocAve can deliver a more potent solution.

AvePoint

Objective #1:   User and Content Management

How can ACME go about making sure that each end user only has access to the sites they are authorized to view and/or modify, and do so in an efficient manner? Additionally, how can users be prevented from uploading content that is not business-appropriate or compliant?

DocAve *SharePoint Administrator* empowers ACME with universal and centralized control over their enterprise-wide SharePoint securities and permissions regime. With DocAve *SharePoint Administrator*, administrators can:

- **Easily view, search, manage, report, and replicate configurations, and security of SharePoint objects and users throughout an entire SharePoint deployment from a single interface.**

- **Discover and target users and objects in tree-mode or returned via a global search engine, and perform actions upon these elements granularly or in bulk with precision and speed.**

- **Automate the process of de-authorizing user accounts via a dynamic "dead account" cleaner.**

- **Easily clone and transfer permissions from one user to another user or group of users.**

- **Execute efficient, rule-based searches and provide diligent management of user security across all hierarchies and object-levels, from both end-user and object perspectives.**

- **Create sophisticated, enterprise-level environmental reports (exportable to multiple formats, including PDF, XML, and CSV) analyzing end user behaviors, administration activity, and platform growth.**

- **Track and archive all administrative actions, and receive real-time email notification of target activities for both on-demand review and audit fulfillment.**
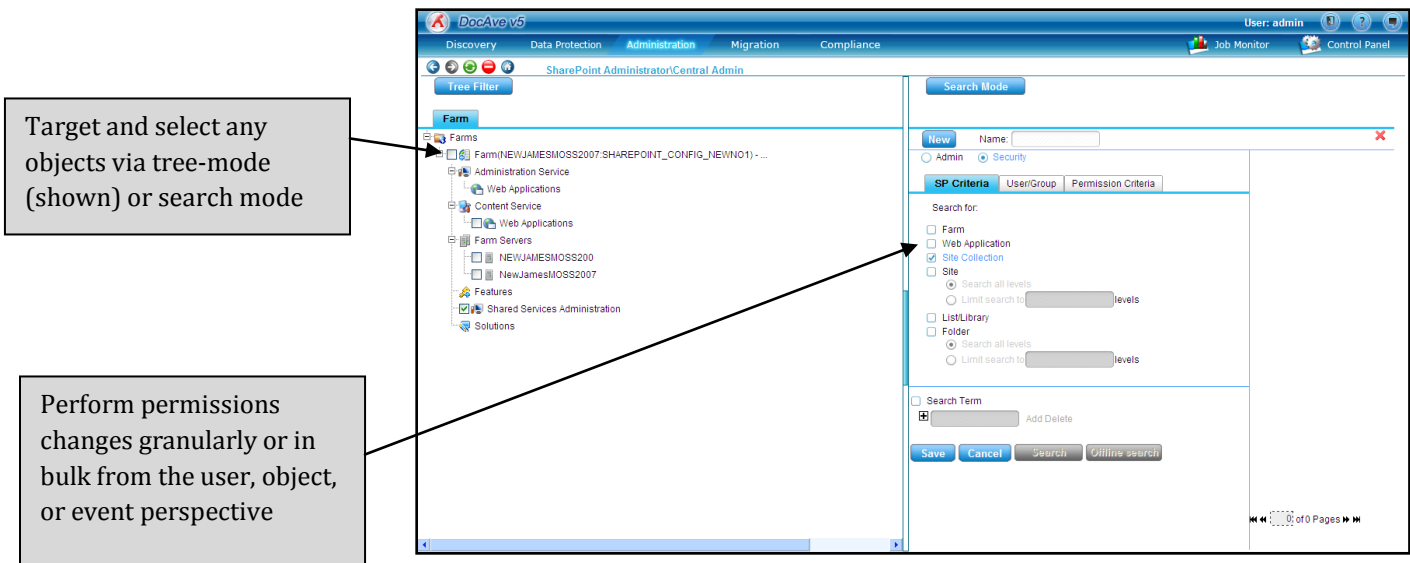
AvePoint

Target and select any objects via tree-mode (shown) or search mode

Perform permissions changes granularly or in bulk from the user, object, or event perspective

Figure 12: DocAve *SharePoint Administrator*

With DocAve *SharePoint Administrato*r, ACME can discover and manage the permissions of a particular user or group throughout the deployment, all from a single interface. They can set, break, or prescribe exclusion rules to inheritance-based permissions for an end-user or group at any level of the deployment hierarchy with precision and speed. This will allow ACME to ensure the confidentiality and integrity of data without burdening IT staff with tedious manual tasks, and will reduce the organizations exposure to human-error and oversight.

DocAve *Content Shield* empowers ACME to pro-actively prevent unauthorized or non-compliant content from being uploaded to SharePoint. DocAve *Content Shield*, regulates the presence of content by any number of attributes, including keyword, metadata tags, and file type – and provides flexible notification functionality to inform administrators when attempts to upload such materials have been made. This gives ACME the assurance that their SharePoint platform remains free of content that is not business-appropriate or compliant.

Doc*Ave eDiscovery* enables ACME to continually scan all SharePoint content – both active and historical – for any keyword, phrase, or metadata tag. Results of these searches are exportable to multiple formats and reports, all delivered with full metadata and audit histories intact. DocAve *eDiscovery* offers fully customizable scheduling of such scans, so ACME can consistently track trends with regard to SharePoint content activity, and make better informed decisions about upload policies. DocAve's flexible report generation and export feature allow ACME to document and affirm its content upload activity in response to any legal or regulatory request.

Objective #2:   **Auditing User and Content Management**

How can ACME audit the access and modification histories of its 100 "regulated" sites, two of which reside in each of its 50 site collections?   Then how can ACME generate reports based upon this audit data in a manner that does not excessively burden IT staff and management?

AvePoint

DocAve *Auditor* provides ACME the precision tools they need to confidently track and record all SharePoint interactions and events - including all usage, searches/queries, and security changes - to proactively satisfy their compliance obligations. User-errors such as unintended deletion of sites, unexpected transfers of site ownership, and unforeseen access right changes can be tracked and identified quickly, minimizing costly non-compliance exposure. To assist in the preparation of responsive materials, DocAve *Auditor* delivers comprehensive, customizable reports of any SharePoint activity based on numerous attributes, including time viewed/modified/deleted/renamed and workflow origin. To facilitate compliance-related monitoring routines, DocAve *Auditor* delivers variable audit control from the site collection-level down to the user or object, and provides customizable data pruning for effective resource management based upon time-range, locations, users, and action types. Unlike SharePoint's native functionality, DocAve *Auditor* will allow ACME to:

- **Audit platform activities from every perspective (i.e. the object, the action, or the particular user/group) and every event (e.g. time viewed/modified/deleted/undeleted/renamed, permission/setting modification, and workflow origination).**

- **Audit the deletion of sites.**

- **Enable granular auditing of site collections, sites, lists, libraries, objects, and users, letting ACME align its auditing procedures with regulatory requirements.**

- **Generate reports at all levels of the platform hierarchy (site collection, site, list, library, and object) and all perspectives (the object-level, the action-level, or a particular user/group-level), for any desired time-frame. These reports can be customized to target only designated events, users, or elements, and no scripted queries must be crafted to deliver these reports.**

Filter auditing by user, object, date-range or discrete activity

Enable auditing and generate reports based on any event criteria, user, or object at any level in the SharePoint hierarchy
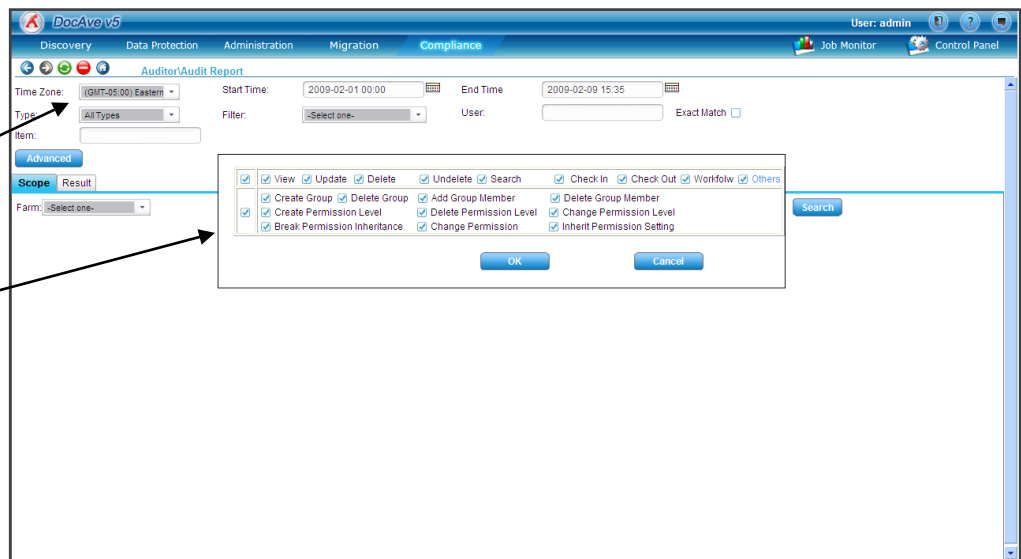

Figure 13: DocAve *Auditor*

Objective #3:   Storing Audit Data

How can ACME store its audit data for 10 years without excessively burdening system resources or performance?

DocAve *Auditor* empowers ACME to meet this obligation in two vital ways: First, as we mentioned in our review of Objective #2, DocAve allows administrators to granularly target the events, users, and/or objects they wish to audit, according to the exact hierarchy level (at the site collection, site, list, library, and object-level) they need, and from every perspective (the object, the action, or the user/group.) Second, DocAve stores this audit data in its own proprietary structured data format (storable on any file system), thereby relieving SharePoint of the burden of hosting this data. As a result, with DocAve, the size of audit data captured can be optimized, and the SharePoint platform itself can dedicate its valuable space and resources to delivering optimal performance.

Maintaining the Availability of Information

We identified three objectives ACME had to meet in order to satisfy its obligations with regard to the availability of information stored in SharePoint. Let's break down each of these objectives, and discuss how DocAve can deliver a more potent solution.

Objective #1:   Platform Availability Management

How can ACME develop, maintain, and document platform reliability, via appropriate platform protection and disaster recovery strategies? How can ACME limit platform configuration access to only those so authorized? How can ACME enable auditing on its platform protection and configuration activities, and generate reports based on this audit data in a timely manner? How can they perform all these requirements in a manner that does not excessively burden IT and management resources?

DocAve *Backup and Recovery*, with item- through platform-level protection, provides fast, reliable backup and restore functionality for your entire SharePoint environment.   By protecting your entire platform – including all server configurations, customizations, content, securities, and metadata - platform recovery times are drastically reduced, the costs associated with such activities are minimized, and the risks associated with manual recovery processes are mitigated.

The flexibility of DocAve *Backup and Recovery* allows for frequent platform-level backups to be executed even during production hours, achieving the lowest possible RPO (Recovery Point Objective). This means up-to-date versions of all SharePoint content, configurations, and components can easily be recovered following accidental deletion, corruption, or DR events. Productivity-loss is minimized by ensuring restoration of the most current data.

AvePoint

DocAve *High Availability* provides the industry's most reliable continuous uptime solution, providing a full 'standby' environment that is easily accessible in the event of data-center or platform architecture-loss. DocAve *High Availability* lets organizations realize absolute minimal downtime following the loss of a production environment.

DocAve *SharePoint Administrator* empowers ACME to efficiently manage all accounts associated with platform-level activity. Via DocAve's role-based *Access Control Interface*, ACME can delegate exactly the authorities required to configure components of the platform. No one need be given the "keys to the kingdom," which unnecessarily exposes the company to confidentiality and availability risk.

DocAve *Auditor* lets ACME confidently track and record all events and activities effecting the protection and configuration of the platform via a single interface, and generate comprehensive, customizable reports based on this activity.

Objective #2: **Active Content Availability Management**

How can ACME develop, maintain, and document protection of its active content? How can ACME enable auditing on its content protection activities, and generate reports based on this audit data in a timely manner? How can ACME search its live content efficiently in response to regulatory and legal requests? How can they perform all these requirements in a manner that does not excessively burden IT and management resources?

DocAve *Backup and Recovery* delivers the full fidelity, item through platform-level data protection ACME requires to ensure the highest possible availability of its SharePoint data and metadata, while ensuring that storage resources are optimized. DocAve's pioneering Criticality Matrix automates the backup-plan building process by granularly classifying all content based upon both business-importance and usage activity, then automatically prescribes it to an appropriate backup schedule based upon user-defined rules. This fully customizable tool lets administrators design rule-based backups for each discrete piece of data within their SharePoint deployment based upon real-time analyses, in order to meet aggressive SLA's without burdening administrators.

- **Unlike reliance on SharePoint's Recycle Bin, DocAve protects ACME from data corruption, by allowing for fast, item-level recovery of data directly to the production environment.**

- **Unlike dependence on SharePoint Versioning, DocAve ensures that platform performance is optimized by offloading backup data off the SharePoint database.**

- **Unlike SQL Server restores, DocAve allows for precision recovery of content at the item-level. This ensures that - should ACME need to recover a single document - doing so will not necessitate the loss of all content and metadata changes that occurred since the last SQL backup was performed.**

AvePoint

DocAve *eDiscovery* will empower ACME to regularly and continually search – in real-time or according to customizable schedules – all live or archived SharePoint content by any combination of keywords, attributes, and metadata fields, to ensure meticulous response to any legal and compliance inquiries. With sophisticated search capabilities - by keyword, attribute, and metadata criteria – DocAve *eDiscovery* accelerates both the targeting and segregation of responsive content. Evidence identified through the discovery process – including not only content, but all metadata and audit history – can be selected and exported to multiple portable and viewable formats, letting external legal authorities review it via their own protocols and/or software platforms. All responsive data is delivered with all applicable metadata, attributes, audit histories, and source locations - via an affiliated .xml, .pdf, or .csv file - to ensure exhaustive compliance, as required. DocAve *eDiscovery* provides a flexible, scalable solution that simplifies electronic content identification, streamlines retrieval & delivery, and diligently prevents future non-compliance instances.

Objective #3:   **Historical Content Availability Management**

How can ACME enable efficient access to historical information when required, in a manner that is not cost-prohibitive and does not excessively burden system resources? How can it make this information available for regulatory or legal review upon request, in an efficient manner?

DocAve *Vault* lets ACME administrators confidently satisfy all compliance-related retention requirements with tools to ensure the proper stewardship of audit data, the stringent enforcement of retention policies, and the successful completion of searches related to legal discoveries, audits, and reviews. With automatic capture of complete and customizable datasets – including all securities and metadata – in an immutable form, administrators can be assured that all compliance-responsive materials are secure and whole. With precision data retrieval based on metadata, full-content, and contextual searches – complimented by tools to conduct relevance ranking, search-term highlighting, and results 'collapsing' – archive data can be targeted and compiled quickly and efficiently. With standardized and customizable reports based on current regulatory protocols, automated data pruning based on administrator-prescribed policies, and random sampling capabilities, DocAve *Vault* significantly reduces risk exposure related to data tampering and unintended data loss.

- Unlike SharePoint's Records Center, data archived by DocAve *Vault* is not stored on SharePoint, thereby relieving its SQL database of cumbersome archive data, and ensuring archive materials are safe even if SharePoint undergoes platform failure.

- DocAve *Vault* lets organizations set archiving rules by any established or customized metadata value, and any user/group, so archiving performance is totally aligned with business needs.

AvePoint

⚔ **Unlike Records Center, DocAve can provide an unlimited number of reports – based on metadata, user, group, keyword, or via random sampling – to satisfy any regulatory and/or legal request.**

Compliance Delivered

As our discussion has revealed, though the goals of IT compliance can be reasonably distilled into a handful of key objectives, meeting these objectives demands procedures that span a diverse array of business operations, and tools that empower the organization to enact these procedures with efficiency.

For organizations running SharePoint, satisfying compliance obligations presents unique challenges. Because of SharePoint's limited capabilities and heavy reliance on tedious manual routines, it simply does not provide the flexibility or potency organizations demand to aggressively meet their compliance challenges.

Powerful solutions such as the **DocAve Governance Suite** provide organizations with the flexible tools required to meet all IT compliance obligations diligently, comprehensively, and efficiently.

AvePoint

Additional Resources

This documents provides only a brief survey of the many compliance obligations an organization running SharePoint might face, and tools available to help satisfy those obligations. The following resources offer additional information and analyses on the subject.

Effective SharePoint Governance
> *A guide to aid IT administrators and other stakeholders responsible for managing Microsoft SharePoint deployments, in planning and implementing a comprehensive, reliable and efficient governance strategy appropriate to their organizational needs.*
> (http://www.avepoint.com/assets/products/Effective_SharePoint_Governance.pdf)

Best Practices for SharePoint Backup and Recovery
> *A white paper to aid IT administrators responsible for managing Microsoft SharePoint deployments in planning and implementing a comprehensive, reliable, and efficient data protection strategy, outlining the planning, guidelines, and implementation considerations for SharePoint backup and disaster recovery, then briefly reviews the singular attributes DocAve Backup and Recovery.*
> (http://www.avepoint.com/assets/sharepoint_whitepapers/Best-Practices-for-SharePoint-Backup-and-Recovery.pdf)

Microsoft IT Compliance Management Guide
> *A guide intended for IT managers and IT professionals to help plan for and address the governance, risk, and compliance requirements of their organizations.*
> (http://www.microsoft.com/downloads/details.aspx?FamilyId=BD930882-0D39-4900-9A79-B91F213ED15D&displaylang=en)

Sarbanes-Oxley Act of 2002
> http://uscode.house.gov/download/pls/15C98.txt

Health Insurance Portability and Accountability Act
> http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/index.html

European Union Data Protection Directive
> http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Title 21 CFR Part 11 of the Federal Food, Drug and Cosmetic Act
> http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=e78493028ca776360c988855f2f0a2dd&rgn=div5&view=text&node=21:1.0.1.1.7&idno=21#21:1.0.1.1.7.2.31.1

International Organization for Standardization
> http://www.iso.org

AvePoint

i SARBANES-OXLEY ACT OF 2002

(Enrolled as Agreed to or Passed by Both House and Senate)

Section 404 -- Management Assessment of Internal Controls

a. Rules Required. The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 to contain an internal control report, which shall--
1. state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
2. contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
b. Internal Control Evaluation and Reporting. With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

(For the complete and most current text of the Sarbanes-Oxley Act of 2002, please visit http://uscode.house.gov/download/pls/15C98.txt.)

ii HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

Public Law 104-191
104th Congress

An Act

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

...

(2) SAFEGUARDS.--Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--
(A) to ensure the integrity and confidentiality of the information;
(B) to protect against any reasonably anticipated--
(i) threats or hazards to the security or integrity of the information; and
(ii) unauthorized uses or disclosures of the information; and
(C) otherwise to ensure compliance with this part by the officers and employees of such person.

...

The Department of Health and Human Services is tasked with providing standards and administrative requirements organizations are to follow in order to comply with HIPAA. Below is a relevant portion of the DHHS' published Administrative Requirements.

HHS recognizes that covered entities range from the smallest provider to the largest, multi-state health plan. Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, as well as the covered entity's size and resources.

Data Safeguards. A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.70 For example, such safeguards might include shredding documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. See OCR "Incidental Uses and Disclosures"

Guidance.

Documentation and Record Retention. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.

(For the complete and most current text of the Health Insurance Portability and Accountability Act, please visit http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/index.html)

(For further information regarding Department for Health and Human Service rules enacted with regard to HIPAA, please visit: http://www.hhs.gov/)

iii DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

...

Article 1 - Object of the Directive
1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2 - Definitions

For the purposes of this Directive:
(a) 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
(b)'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;
(d)'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;
(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
(h)'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3 Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:
· in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,
· by a natural person in the course of a purely personal or household activity.

Article 6

1. Member States shall provide that personal data must be:
    (a) processed fairly and lawfully;
    (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
    (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
    (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
    (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
2. It shall be for the controller to ensure that paragraph 1 is complied with.

[iv] 21 U.S.C. 321–393; 42 U.S.C. 262.

Subpart A—General Provisions
§ 11.1 Scope.
 (a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.
(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.
(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with §11.2, unless paper records are specifically required.
(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.
(f) This part does not apply to records required to be established or maintained by §§1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.
[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004]
§ 11.2 Implementation.
 (a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.
(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:
(1) The requirements of this part are met; and
(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.
§ 11.3 Definitions.
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.
(b) The following definitions of terms also apply to this part:
(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).
(2) *Agency* means the Food and Drug Administration.
(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B—Electronic Records

§ 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

…

(For the complete and most current text of Title 21 CFR Part 11 of the Federal Food, Drug and Cosmetic Act, please visit http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=e78493028ca776360c988855f2f0a2dd&rgn=div5&view=text&node=21:1.0.1.1.7&idno=21#21:1.0.1.1.7.2.31.1)

The U.S. Food and Drug Administration (FDA) is tasked with enforcing Title 21 CFR Part 11 of the Federal Food, Drug, and Cosmetic Act. the following is an excerpt of guidelines published by the FDA, to assist organizations attempting to comply with Title 21 CFR Part 11:

"It is important to note that FDA's exercise of enforcement discretion as described in this guidance is limited to specified part 11 requirements (setting aside legacy systems, as to which the extent of enforcement discretion, under certain circumstances, will be more broad). We intend to enforce all other provisions of part 11 including, but not limited to, certain controls for closed systems in § 11.10. For example, we intend to enforce provisions related to the following controls and requirements:

- · limiting system access to authorized individuals
- · use of operational system checks
- · use of authority checks
- · use of device checks
- · determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- · establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- · appropriate controls over systems documentation
- · controls for open systems corresponding to controls for closed systems bulleted above (§ 11.30)
- · requirements related to electronic signatures (e.g., §§ 11.50, 11.70, 11.100, 11.200, and 11.300)

2. Audit Trail

The Agency intends to exercise enforcement discretion regarding specific part 11 requirements related to computer-generated, time-stamped audit trails (§ 11.10 (e), (k)(2) and any corresponding requirement in §11.30). Persons must still comply with all applicable predicate rule requirements related to documentation of, for example, date (e.g., § 58.130(e)), time, or sequencing of events, as well as any requirements for ensuring that changes to records do not obscure previous entries.

Even if there are no predicate rule requirements to document, for example, date, time, or sequence of events in a particular instance, it may nonetheless be important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the records.[6] We recommend that you base your decision on whether to apply audit trails, or other appropriate measures, on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and safety and record integrity. We suggest that you apply appropriate controls based on such an assessment. Audit trails can be particularly appropriate when users are expected to create, modify, or delete regulated records during normal operation.

The Agency intends to exercise enforcement discretion with regard to the part 11 requirements for the protection of records to enable their accurate and ready retrieval throughout the records retention period (§ 11.10 (c) and any corresponding requirement in §11.30). Persons must still comply with all applicable predicate rule requirements for record retention and availability (e.g., §§ 211.180(c),(d), 108.25(g), and 108.35(h)).
We suggest that your decision on how to maintain records be based on predicate rule requirements and that you base your decision on a justified and documented risk assessment and a determination of the value of the records over time.

FDA does not intend to object if you decide to archive required records in electronic format to nonelectronic media such as microfilm, microfiche, and paper, or to a standard electronic file format (examples of such formats include, but are not limited to, PDF, XML, or SGML). Persons must still comply with all predicate rule requirements, and the records themselves and any copies of the required records should preserve their content and meaning. As long as predicate rule requirements are fully satisfied and the content and meaning of the records are preserved and archived, you can delete the electronic version of the records. In addition, paper and electronic record and signature components can co-exist (i.e., a hybrid[8] situation) as long as predicate rule requirements are met and the content and meaning of those records are preserved.

According to Part 11 §11.10 (e) audit trails must be secure, computer-generated and time-stamped to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. Audit trails should say 'who did what to your records and when (why for GLP)'. Part 11 does not specify the format for audit trials. This should be discussed in a forthcoming FDA guidance document for Part 11 audit trails.

[v] **ISO/IEC 27002:2005** is a several hundred page document establishing standards for information security management. As such, the following represents only a brief summary of the standard's sections. (This summary provided by www.iso27001security.com)

Section 1: Scope
The standard gives information security management recommendations for those who are responsible for initiating, implementing or maintaining security.

Section 2: Terms and definitions
"Information security" is explicitly defined as the "preservation of confidentiality, integrity and availability of information". These and other related terms are further defined. [In due course when ISO/IEC 27000 has been released and ISO/IEC 27002 is revised, this section will presumably reference definitions in ISO/IEC 27000.]

Section 3: Structure of this standard
This page simply explains that the guts of the standard contain control objectives, suggested controls and implementation guidance.

Section 4: Risk assessment and treatment
The current ISO/IEC 27002 standard covers the topic of risk management in just a page and a half, woefully inadequate coverage for such a complex and central element of information security. [When ISO/IEC 27002 is revised, it will probably reference ISO/IEC 27005. In keeping with the style of ISO/IEC 27002, ISO/IEC 27005 gives general guidance on selecting and using appropriate methods to analyze information security risk - it does not mandate a specific method since 'appropriate' depends on context.]

Section 5: Security policy
Management should define a policy to clarify their direction of, and support for, information security, meaning a short, high-level information security policy statement laying down the key information security directives and mandates for the entire organization. This is normally supported by a comprehensive suite of more detailed corporate information security policies, typically in the form of an information security policy manual. The policy manual in turn is supported by a set of information security standards, procedures and guidelines.
Although the standards are somewhat ambiguous on this point, the information security policy noted in ISO/IEC 27002 is generally understood to be separate and different from the ISMS policy required by ISO/IEC 27001. The ISMS policy is seen by some as a strategy or governance paper laying out management's support for the ISMS as a whole.

Section 6: Organization of information security
A suitable information security governance structure should be designed and implemented.
6.1 Internal organization
The organization should have a management framework for information security. Senior management should provide direction and commit their support, for example by approving information security policies. Roles and responsibilities should be defined for the information security function. Other relevant functions should cooperate and coordinate their activities. IT facilities should be

authorized. Confidentiality agreements should reflect the organization's needs. Contacts should be established with relevant authorities (*e.g.* law enforcement) and special interest groups. Information security should be independently reviewed.

6.2 External parties

Information security should not be compromised by the introduction of third party products or services. Risks should be assessed and mitigated. when dealing with customers and in third party agreements.

Section 7: Asset management

The organization should be in a position to understand what information assets it holds, and to manage their security appropriately.

7.1 Responsibility for assets

All [information] assets should be accounted for and have a nominated owner. An inventory of information assets (IT hardware, software, data, system documentation, storage media, supporting assets such as computer room air conditioners and UPSs, and ICT services) should be maintained. The inventory should record ownership and location of the assets, and owners should identify acceptable uses.

7.2 Information classification

Information should be classified according to its need for security protection and labeled accordingly. [While this is clearly most relevant to military and government organizations handling 'protectively marked information' (Top Secret *etc.*), the concept of identifying important assets, classifying/grouping them, and applying controls that are judged suitable for assets of that nature, is broadly applicable.]

Section 8: Human resources security

The organization should manage system access rights *etc.* for 'joiners, movers and leavers', and should undertake suitable security awareness, training and educational activities.

8.1 Prior to employment

Security responsibilities should be taken into account when recruiting permanent employees, contractors and temporary staff (*e.g.* through adequate job descriptions, pre-employment screening) and included in contracts (*e.g.* terms and conditions of employment and other signed agreements on security roles and responsibilities).

8.2 During employment

Management responsibilities regarding information security should be defined. Employees and (if relevant) third party IT users should be made aware, educated and trained in security procedures. A formal disciplinary process is necessary to handle security breaches.

8.3 Termination or change of employment

Security aspects of a person's exit from the organization (*e.g.* the return of corporate assets and removal of access rights) or change of responsibilities should be managed.

Section 9: Physical and environmental security

Valuable IT equipment should be physically protected against malicious or accidental damage or loss, overheating, loss of mains power *etc.*

9.1 Secure areas

This section describes the need for concentric layers of physical controls to protect sensitive IT facilities from unauthorized access.

9.2 Equipment security

Critical IT equipment, cabling and so on should be protected against physical damage, fire, flood, theft *etc.*, both on- and off-site. Power supplies and cabling should be secured. IT equipment should be maintained properly and disposed of securely.

Section 10: Communications and operations management

This lengthy, detailed section of the standard describes security controls for systems and network management.

10.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Duties should be segregated between different people where relevant (*e.g.* access to development and operational systems should be segregated).

10.2 Third party service delivery management

Security requirements should be taken into account in third party service delivery (*e.g.* IT facilities management or outsourcing), from contractual terms to ongoing monitoring and change management. Do you have suitable security clauses in the contract with your ISP?

10.3 System planning and acceptance

Covers IT capacity planning and production acceptance processes.

10.4 Protection against malicious and mobile code

Describes the need for anti-malware controls, including user awareness. Security controls for mobile code 'associated with a number of middleware services' are also outlined.

10.5 Back-up

Covers routine data backups and rehearsed restoration.

10.6 Network security management

Outlines secure network management, network security monitoring and other controls. Also covers security of commercial network services such as private networks and managed firewalls *etc.*

10.7 Media handling

Operating procedures should be defined to protect documents and computer media containing data, system information *etc.* Disposal of backup media, documents, voice and other recordings, test data *etc.* should be logged and controlled. Procedures should be defined for securely handling, transporting and storing backup media and system documentation.

10.8 Exchange of information

Information exchanges between organizations should be controlled, for example though policies and procedures, and legal agreements. Information exchanges should also comply with applicable legislation. Security procedures and standards should be in place to protect information and physical media *in transit*, including electronic messaging (email, EDI and IM) and business information systems.

10.9 Electronic commerce services

The security implications of eCommerce (online transaction systems) should be evaluated and suitable controls implemented. The integrity and availability of information published online (*e.g.* on websites) should also be protected.

10.10 Monitoring

Covers security event/audit/fault logging and system alarm/alert monitoring to detect unauthorized use. Also covers the need to secure logs and synchronize system clocks.

Section 11: Access control

Logical access to IT systems, networks and data must be suitably controlled to prevent unauthorized use. This is another lengthy and detailed section.

11.1 Business requirement for access control

The organization's requirements to control access to information assets should be clearly documented in an access control policy, including for example job-related access profiles (role based access control). [This is an important obligation for information asset owners.]

11.2 User access management

The allocation of access rights to users should be formally controlled through user registration and administration procedures (from initial user registration through to removal of access rights when no longer required), including special restrictions over the allocation of privileges and management of passwords, and regular access rights reviews.

11.3 User responsibilities

Users should be made aware of their responsibilities towards maintaining effective access controls *e.g.* choosing strong passwords and keeping them confidential. Systems and information should be secured when left unattended (*e.g.* clear desk and clear screen policies).

11.4 Network access control

Access to network services should be controlled, both within the organization and between organizations. Policy should be defined and remote users (and possibly equipment) should be suitably authenticated. Remote diagnostic ports should be securely controlled. Information services, users and systems should be segregated into separate logical network domains. Network connections and routine should be controlled where necessary. [See also ISO/IEC 27033]

11.5 Operating system access control

Operating system access control facilities and utilities (such as user authentication with unique user IDs and managed passwords, recording use of privileges and system security alarms) should be used. Access to powerful system utilities should be controlled and inactivity timeouts should be applied.

11.6 Application and information access control

Access to and within application systems should be controlled in accordance with a defined access control policy. Particularly sensitive applications may require dedicated (isolated) platforms, and/or additional controls if run on shared platforms.

11.7 Mobile computing and teleworking

There should be formal policies covering the secure use of portable PCs, PDAs, cellphones *etc.*, and secure teleworking ("working from home", "road warriors" and other forms of mobile or remote working).

Section 12: Information systems acquisition, development and maintenance

Information security must be taken into account in the processes for specifying, building/acquiring, testing, implementing and maintaining IT systems.

12.1 Security requirements of information systems

Automated and manual security control requirements should be analyzed and fully identified during the requirements stage of the systems development or acquisition process, and incorporated into business cases. Purchased software should be formally tested for security, and any issues risk-assessed.

12.2 Correct processing in application systems

Data entry, processing and output validation controls and message authentication should be provided to mitigate the associated integrity risks.

12.3 Cryptographic controls

A cryptography policy should be defined, covering roles and responsibilities, digital signatures, non-repudiation, management of keys and digital certificates *etc.*

12.4 Security of system files

Access to system files (both executable programs and source code) and test data should be controlled.

12.5 Security in development and support processes

Application system managers should be responsible for controlling access to [development] project and support environments. Formal change control processes should be applied, including technical reviews. Packaged applications should ideally not be modified. Checks should be made for information leakage for example *via* covert channels and Trojans if these are a concern. A number of supervisory and monitoring controls are outlined for outsourced development.

12.6 Technical vulnerability management

Technical vulnerabilities in systems and applications should be controlled by monitoring for the announcement of relevant security vulnerabilities, and risk-assessing and applying relevant security patches promptly.

Section 13: Information security incident management

Information security events, incidents and weaknesses (including near-misses) should be promptly reported and properly managed.

13.1 Reporting in information security events and weaknesses

An incident reporting/alarm procedure is required, plus the associated response and escalation procedures. There should be a central point of contact, and all employees, contractors *etc.* should be informed of their incident reporting responsibilities.

13.2 Management of information security incidents and improvements

Responsibilities and procedures are required to manage incidents consistently and effectively, to implement continuous improvement (learning the lessons), and to collect forensic evidence.

Section 14: Business continuity management

This section describes the relationship between IT disaster recovery planning, business continuity management and contingency planning, ranging from analysis and documentation through to regular exercising/testing of the plans. These controls are designed to minimize the impact of security incidents that happen despite the preventive controls noted elsewhere in the standard.

Section 15: Compliance

15.1 Compliance with legal requirements

The organization must comply with applicable legislation such as copyright, data protection, protection of financial data and other vital records, cryptography restrictions, rules of evidence *etc*.

15.2 Compliance with security policies and standards, and technical compliance

Managers and system owners must ensure compliance with security policies and standards, for example through regular platform security reviews, penetration tests *etc*. undertaken by competent testers.

15.3 Information systems audit considerations

Audits should be carefully planned to minimize disruption to operational systems. Powerful audit tools/facilities must also be protected against unauthorized use.

(To learn more about ISO/IEC 27002:2005, and to access the guideline in full, please visit http://www.iso.org/)

For AvePoint Products and Services, please visit our website at www.avepoint.com.

AvePoint