



Addressing Compliance Requirements with Xythos Technology

Table of Contents

Overview	1
The Inescapability of Compliance	1
The Fundamental Compliance Challenge	1
Compliance and BCS.....	2
From Collaboration to BCS to Compliance	2
How Xythos Can Help	2
Xythos Products	2
Server products	3
Desktop tools.....	3
Addressing Compliance with Xythos Features	4
Integration and Customization	10
Common Customizations	10
Putting It All Together	12
Xythos and Sarbanes-Oxley	12
Overview	12
Collecting, sharing, and reviewing internal controls	12
Features used.....	13
Xythos and HIPAA	13
Overview	13
HIPAA and human subjects.....	14
Features used.....	15
Conclusion	15

Overview

Compliance has become an inescapable part of daily life. This whitepaper examines how online document management may assist organizations to improve collaboration, manage and secure sensitive data, reduce duplication and errors and provide audit processes for all documents.

The Inescapability of Compliance

Compliance has become an inescapable part of daily life. While some of the initial press around new standards like Sarbanes-Oxley and HIPAA may have exaggerated the scope and burden of compliance requirements somewhat, it's hard to escape compliance, no matter what your job. Here are just a few examples:

- Public corporations must adhere to older SEC regulations about financial reporting, plus the newer Sarbanes-Oxley rules that have expanded the demand for accountability and transparency.
- Universities must follow federal FERPA guidelines to protect the privacy of student information.
- The Department of Defense's records management standard, DoD 5015.2, is widely adopted throughout the federal government and corporations that do business with it.
- Because of HIPAA, not only do health care practitioners need to protect the private details of a patient's medical conditions, but every human resources department has the same concerns about any medical-related information they may have about employees.
- State, county, and local governments enact their own guidelines that may expand on federal guidelines concerning the privacy of personal data, the accessibility of information about public and private institutions within their jurisdictions, and other compliance requirements.

And that's just the United States. In global businesses, corporations must adhere to accounting standards like Basel II. Public and private organizations apply the ISO best practices standards, such as ISO 17799 (a.k.a. BS 7799), which lays down guidelines for information security. Europe has its own records management standard, the Model Requirements for Management of Electronic Records (MoReq) that mirrors the functionality required in DoD 5015.2.

It should be no surprise, therefore, that organizations find themselves wrestling with an increasing number of compliance requirements. If these requirements were all the same type, compliance might be a simple matter of building an all-embracing system to handle all electronic information that would be subject to these rules. Unfortunately, the standards themselves are very different, complicating compliance even further.

The Fundamental Compliance Challenge

Anyone who has read an article about compliance has already heard a familiar refrain about what makes compliance difficult. Organizations have to make new IT investments, such as additional layers of backup and security. Users have to change their work habits to meet new and changing compliance requirements. Demonstrating compliance can easily turn into a new job for many employees, cutting into the time available to perform their regular job.

Therefore, organizations will invest in any mechanisms that make compliance easier, such as specialized applications that help users to understand and follow the rules. Organizations also want to exert some remote control over users, so that they can't avoid following these rules. Ironically, both of these measures, specialization and automation, can work against compliance. The more unfamiliar a system is, the less likely users will adopt it. The more "remote control" managers try to exert over their employees, the more resistant to these

obnoxious measures the employee will become. Not surprisingly, the Gartner Group ranks user rejection and indifference as the chief compliance challenge today.

Compliance and BCS

Compliance shapes many aspects of how an organization operates, including how it manages its IT systems. Now that compliance requirements are ubiquitous, users and managers alike are concerned about the costs imposed, both by using compliance systems and by not using them. A company's finance division may not be able to do its regular work if Sarbanes-Oxley and other financial reporting requirements consume all available time. A hospital may have to hire extra staff just to help doctors and nurses enter information into a HIPAA application. At the same time, commercial firms know the steep penalties for failing to comply with Sarbanes-Oxley, and hospitals recognize the risk of litigation if they accidentally divulge patient information to the wrong people.

Happily, the ecology of IT has evolved to the point where these choices are much less painful. Several years ago, the choice was among:

- File management tools, which lacked many of the features (auditing, workflow, etc.) needed to meet compliance requirements;
- Collaboration tools, which may have had a few of these features, but which often lacked security and other features required; and
- High-end document management systems, which were often too expensive to deploy, and too difficult for the average employee to use.

A fourth niche—something with more DM-like functionality than file management, more security than collaboration tools, and more usability than traditional DM—was needed. Not surprisingly, the IT ecology evolved to meet this new demand.

Gartner Group calls this new category of software applications, *Basic Content Services*, which might also be referred to as "document management for the rest of us." It builds on the familiarity of file management interfaces (for example, files and folders), the sex appeal of collaboration tools (which help users get their jobs done faster and more effectively), and the subset of DM functionality that organizations need to impose business rules, whether or not these rules are legal or regulatory mandates. (Even if no compliance requirements existed, organizations would want to influence or control how their users create, categorize, secure, update, and destroy electronic documents.)

From Collaboration to BCS to Compliance

In short, Basic Content Services (BCS) are a precursor to compliance. If the tools available to the average user do not help that person identify specific categories of business documents, and then apply the appropriate rules to them, compliance is too far a stretch from the electronic information with which they can barely keep pace already.

Fortunately, the lighter-weight BCS version of traditional DM features is helpful to individuals, not just to the anonymous corporate entity or flesh-and-blood government auditors. This short step from *what helps me* to *what helps the organization* is the transition from collaboration to BCS.

How Xythos Can Help

Xythos Products

A full description of the Xythos product line is available on the main Xythos web site, www.xythos.com. However, a brief summary of these products can better frame how Xythos can help organizations address compliance requirements.

SERVER PRODUCTS

Xythos provides both a development platform and applications built on that platform:

- **WebFile Server:** A set of APIs that provide everything from basic file management to more sophisticated BCS functionality, such as versioning, categorization, and workflow. Xythos used these APIs to build its applications; the same APIs are available for either customizing these applications or building new ones. The WebFile Server provides WebDAV access to the contents of the server. Beneath the Java layer, a relational database stores all information about the system. The actual documents it manages can be stored in the database or, more commonly, in a separate storage device. The system is designed to let customers choose their preferred application server, database, and storage configuration.
- **Enterprise Document Manager:** An application that Xythos developed on the WebFile System platform. This application exposes file management, collaboration, and BCS features in a way that any person in any organization can use. The actual functionality beneath the application, in the WebFile System platform, may be broader than what the application itself exposes. For example, the security-related APIs provide more options (for example, integration with server-side encryption tools) than the out-of-the-box application provides. This approach lets any set of users get started with the general-purpose features, and then shape them to fit their specific requirements through customization, if strictly needed. The Enterprise Document Manager includes a web UI, portlets, and basic access through WebDAV clients (for example, the Web Folders portion of Microsoft Explorer).
- **Digital Locker:** The same application as the Enterprise Document Manager, minus a few BCS features (workflow, retention rules, document categorization, and custom metadata tied to document categories). The Digital Locker is designed for customers who want document collaboration now, but may not need full-blown BCS capabilities right away.

DESKTOP TOOLS

Xythos also provides a utility that brings BCS more directly to the Windows desktop. The Xythos Drive extends Microsoft Explorer in three important ways:

- **Improved WebDAV support:** The WebDAV standard was designed for secure document collaboration and file management across the Internet. Unfortunately, the operating system-level implementations of WebDAV have some key deficiencies. For example, Microsoft's Web Folders let you double-click and open a file only if it is a Microsoft Office document, and you are opening it in one of Microsoft's editors. The Xythos Drive therefore expands the support for all document formats and all standard file system operations on them.
- **BCS features:** Since the standard Windows, Macintosh, or Linux desktop does not have the BCS features available on the Xythos server (versioning, subscriptions, etc.), the Xythos Drive makes these features available to the desktop user.
- **Better work habits:** Some capabilities of the Xythos Drive are designed to help users better manage their documents. For example, the "offline mode" lets a user work while disconnected, using the same drive mapping that normally connects to the Xythos server. This feature radically simplifies the questions user face about handling documents when working offline. The Xythos Drive synchronizes changes between the local cache and the server when reconnecting, so the user does not have to remember to upload files edited while offline. Similarly, features in the Xythos Drive can intercept email attachments, replacing them with a secure link to an uploaded copy of the file on the Xythos server.

These features help users meet their own needs, such as continuing to work on documents even when an Internet connection is not available. The Xythos Drive's capabilities can also help address compliance requirements, as we'll see in the next section.

Addressing Compliance with Xythos Features

Nearly all Xythos features have a compliance application. The following table shows how some of these features address particular compliance requirements.

ADDRESSING COMPLIANCE WITH XYTHOS FEATURES						
Feature	Description	Sample compliance usage	Availability in Xythos products			
			Xythos Drive	Enterprise Document Manager	Digital Locker	WebFile Server
File management						
WebDAV access (OS)	Access Xythos directly, using the WebDAV implementations in the Windows or Macintosh operating systems, or a UNIX/Linux WebDAV utility.	Without installing special software, Sarbanes-Oxley auditors can see all documents a company has collected to satisfy its reporting requirements.		X	X	X
WebDAV access (Xythos Drive)	Access through the Xythos Drive, letting users map a drive, double-click on documents of any format to open the corresponding editor/viewer, and use BCS features not found in the operating system.	A medical researcher can right-click a document to check in a new version, maintaining the version history needed to satisfy 21 CFR Part 11 requirements.	X	X	X	X
Browser access	Users can upload, access, and manage content through the web UI, delivered through the secure version of HTTP.	Following ISO 17799 recommendations, users whose desktops and laptops have severe restrictions on what software they can run, or how they log into the local operating system, can still manage documents through the web UI.		X	X	
Off-line access	The Xythos Drive provides a way to present the same files and folders, whether the user is connected or disconnected.	A corporate CFO can finish drafting quarterly earnings report while traveling, connect to the server, and automatically upload the changes without having to remember which document needs to be uploaded to which folder on the server.	X			
Intellitach	The system intercepts email attachments, uploads the attached files to the server, and replaces the attachments in the email with secure links to the uploaded documents.	Documents that contain private medical information are never sent as email attachments, which can be forwarded to an unknowable number of other recipients.	X			
URL referenceability	Any document in Xythos can be accessed through a URL, with security enforced on that link.	Adhering to ISO 17799 recommendations about secure protocols, users never open documents through an insecure protocol like SMB/CIFS or	X	X	X	X

ADDRESSING COMPLIANCE WITH XYTHOS FEATURES						
Feature	Description	Sample compliance usage	Availability in Xythos products			
			Xythos Drive	Enterprise Document Manager	Digital Locker	WebFile Server
File management						
		FTP, but only through the secure version of HTTP.				
Working on "live" documents						
Versioning	The system can store new versions of a document as users save them, or when they explicitly check in changes. This feature can be turned on by default for all documents in a folder, or left to users to turn on or off as needed.	By turning versioning on by default in a folder, the system helps medical researchers address CFR 21 Part 11 guidelines about preserving the history of document changes.	X	X	X	X
Logging	The system records when users have created, viewed, edited, or deleted documents. Logging can be turned on by default for all documents in a folder, or left to users to turn on or off as needed.	A company can show Sarbanes-Oxley auditors the record of people who have viewed or changed documents concerning corporate finances.	X	X	X	X
Alerts	The system sends an alert to a subscribed user whenever new documents are created in a folder, documents are deleted from a folder, or documents are viewed or edited.	A human resources professional receives an alert whenever someone accesses personnel documents that might contain HIPAA-governed information.	X	X	X	X
Categorization (general)	Documents can belong to a particular category (a document class), with category-specific metadata and retention rules. The document class may be assigned by default, or users may categorize documents themselves.	Members of the accounting staff can identify any policy and procedures document, regardless of where it is stored, making it easier to collect all internal controls documents for Sarbanes-Oxley auditors.	X	X		X
Enforced categorization	Users uploading documents may be required to assign them to categories, or these categories may be applied by default.	When uploading self-reports required as part of a drug trial, a test subject will have to choose between documents that contain personal information (which a trial administrator must then redact) and documents that contain no identifying information.	X	X		X
Custom metadata (structured)	Document classes have a particular set of attributes, which	Anyone submitting documents to Xythos used as a MoReq-compliant	X	X		X

ADDRESSING COMPLIANCE WITH XYTHOS FEATURES						
Feature	Description	Sample compliance usage	Availability in Xythos products			
			Xythos Drive	Enterprise Document Manager	Digital Locker	WebFile Server
File management						
	may have different datatypes, default values, values limited to a pick list, and required values.	records management system must fill out the metadata required.				
Custom metadata (free-form)	Users can enter any keywords that help later identify a document.	During a legal discovery, the people looking for all documents related to ongoing litigation use these freeform values as yet another way to identify documents that must be included in the discovery.	X	X	X	X
Workflow (approvals and routing)	Workflows automate the approval process, including users whose approval is mandatory or optional. These workflows can also be used when users must acknowledge that they have read and understood a document.	One workflow preserves the list of HR people who approved the manual detailing policies for HIPAA and ADA compliance, while another workflow preserves the list of managers who acknowledge reading the manual.	X	X	X	X
Workflow-driven alerts	Users receive email notifications when the workflow begins, when they approve or reject, when the workflow is reaching a deadline, and when it is completed.	People involved in the mandatory review of research protocol documents receive reminders that they need to approve or reject the documents.		X	X	X
Retention rules	Users or applications can set the retention period of a document. Ownership of the document changes when the retention rule is applied, and the new owner receives notification when the retention period has expired.	A college administrator sees a list of student documents that, according to FERPA guidelines, need to be deleted at some point after graduation.	X	X		X
Expiration	Users or applications can set the length of time before the document expires. By searching for expired documents, users can then identify documents that require updating or other kinds of attention.	A CFO can set policies and procedures documents to expire after a year, ensuring that they receive the kind of regular updates that Sarbanes-Oxley auditors will expect the company to do.	X	X		X
Security						
ACL-based security	Users and groups can be granted permission on a	Following SEC and Sarbanes-Oxley requirements, users in the	X	X	X	X

ADDRESSING COMPLIANCE WITH XYTHOS FEATURES						
Feature	Description	Sample compliance usage	Availability in Xythos products			
			Xythos Drive	Enterprise Document Manager	Digital Locker	WebFile Server
File management						
	document, including read, write, delete, and administer (a variety of options, such as starting a workflow on a document, not available to users with read/write access only).	accounting department can ensure that no one can see documents related to an earnings report before they are completed and ready for publication.				
Tickets	Users can generate a URL that temporarily grants access to a file or folder. Access ends after the defined period, and the link can be password-protected. This mechanism works for users who do not have accounts on the system, as well as those who do.	If authorized by the patient, a doctor at one hospital can share medical records with a colleague at another hospital, without emailing the documents, adding the second doctor to the hospital's LDAP service, or making the document public.	X	X	X	X
Inherited security	Documents in a folder can automatically have the ACLs, automatic logging, and automatic versioning set at the folder level.	As part of the internal controls on financial documents, no one in the accounting staff can upload a document to the Q2 earnings folder without applying a specific set of permissions to a specific set of users, creating an audit trail of activity on the document, and saving all drafts of it.	X	X	X	X
LDAP integration	The users and groups in the Xythos server are defined in the organization's LDAP service. Access to Xythos can be limited to particular groups or individual users.	A company can demonstrate to Sarbanes-Oxley auditors that they maintain a single list of users and groups, and then limit access to the system containing financial documents to the members of the Finance department.	X	X	X	X
Virus scanning	Desktop anti-virus tools work automatically against any mapped drive. Additionally, server-side anti-virus tools can identify and remove infected files behind the scenes.	Universities can demonstrate that multiple layers of anti-virus protection surround student records that are subject to FERPA requirements.	X	X	X	X
Encryption (client tools)	Desktop integration tools can encrypt and decrypt content stored on the Xythos server.	The human resources staff can encrypt personnel documents that may contain private medical information.	X	X	X	X
Digital signatures	With standard tools	Medical researchers can add	X	X	X	X

ADDRESSING COMPLIANCE WITH XYTHOS FEATURES						
Feature	Description	Sample compliance usage	Availability in Xythos products			
			Xythos Drive	Enterprise Document Manager	Digital Locker	WebFile Server
File management						
(documents)	like Adobe Acrobat, users can affix a non-disputable electronic signature to documents. (Since any file stored on the Xythos server is "just a file," the system does not interfere with this process.)	an electronic signature to research protocol documents that are centrally stored, shared, and managed by the research team.				
Finding and collecting documents						
Search: content	Users can quickly search textual content in documents, using a pre-generated index.	During legal discovery, the people collecting documents can find all mentions of a particular person, product, or company involved in the litigation, regardless of the filenames or the folders in which they are stored.		X	X	X
Search: standard attributes	The system stores and manages the standard attributes (Date Created, Date Last Modified, etc.) used in a file system.	After the content has migrated from departmental file servers, standard computer forensics methods, such as looking at the Date Last Modified attribute, work as before.	X	X	X	X
Search: custom attributes (structured)	Users can search on the metadata attached to a particular category of documents (a document class).	During an electronic discovery process, corporate counsel can search for all documents related to XYZ Corporation that have been approved for release to that customer.	X	X		X
Search: custom attributes (free-form)	Users can search on the free-form metadata that users or applications have added to any type of document or folder.	During an electronic discovery process, corporate counsel can search for any extra identifying information that users have added.	X	X	X	X
Ownership/content administration	Files and folders automatically have ownership assigned to them, identifying the users who can effectively administer this content.	Medical researchers can demonstrate that the only users who, by default, can change versioning settings on documents are their owners.	X	X	X	X
Technical architecture						
Server scalability	The system can scale to very large numbers of users and documents, and can handle high rates of concurrency and throughput.	By having a single system where every user and application puts documents, collecting all the internal control documents required under section 404 of the Sarbanes-Oxley Act takes vastly less time than digging through multiple file servers and other systems.		X	X	X
Server reliability	System admins can use standard high-	While the deadline to collect the documentation for a		X	X	X

ADDRESSING COMPLIANCE WITH XYTHOS FEATURES						
Feature	Description	Sample compliance usage	Availability in Xythos products			
			Xythos Drive	Enterprise Document Manager	Digital Locker	WebFile Server
File management						
	availability techniques to ensure a very high rate of reliability.	Sarbanes-Oxley audit gets closer, the financial department does not have to worry about the system not being available.				
Modularity: application server	System admins can change which application server they use in this tier of Xythos, and they can put in place redundant instances to ensure scalability and performance.	As an increasing number of researchers use the same Xythos instance for their projects, the IT staff can upgrade the dedicated application server (with specific security configurations) to handle this expanded usage.		X	X	X
Modularity: database	System admins can change which database they use in this tier of Xythos, and they can use standard database reliability, scalability, security, and recovery features.	In case of a natural disaster, a hospital can recover all patient records, as required by HIPAA.		X	X	X
Modularity: storage	System admins can store files in the database, or they can separate file storage into any standard configuration (SAN, NAS, etc.). Administrators can configure the system to maintain automatic, temporary backups of files, as an extra layer of disaster recovery.	Administrators can use a combination of the Xythos backup and standard file system backup tools to ensure all drug development documentation required by 21 CFR Part 11 is safe in case of system failures, natural disasters, user error, or malicious users.		X	X	X
Standards-based APIs	The APIs used to build specialized applications on the WebFile Server platform, or to customize the Enterprise Document Manager and Digital Locker applications, are Java-based and J2EE compliant. WebDAV provides another standard API for many operations that may need to be controlled through an application.	Once the IT staff has customized an instance of Xythos to further automate HIPAA enforcement, these developers can immediately reuse these skills to add further automation of Sarbanes-Oxley compliance.		X	X	X

Except for that last point, we have been discussing everything that Xythos can do without any coding. However, the Xythos APIs are an important part of the compliance story, since organizations may want to go beyond the capabilities we already provide. This extra layer of insurance that the system meets compliance standards—not to mention the organization's

own business rules—is something that Xythos leaves to the customer to decide. Happily, the robust, standards-based APIs largely remove technological obstacles from building this additional insurance.

Integration and Customization

The previous section demonstrates how Xythos' out-of-the-box products can immediately address compliance needs. However, no system, no matter how well-designed, will be a good long-term investment for compliance if it can't integrate with other compliance-related systems. For example, a research hospital may have built a central metadata repository that includes all the HIPAA codes describing patient conditions. If the BCS system is so inflexible that it can't be integrated with this repository, the work involved in re-creating the same codes all over again in the BCS application may not be worth the effort.

If integration is important, customizability is even more critical to the success of any BCS system used for compliance, for the following reasons:

- **Changes in the standards:** Sometimes, the changes are obvious, such as when legislatures change or add rules. The Sarbanes-Oxley Act, which expanded and amended SEC Rules 17-a3 and 17-a4, is a good example.
- **Changes in the interpretation or enforcement of standards:** Often, the changes are more subtle, when the interpretation and application of the rules changes over time. For example, Sarbanes-Oxley auditors gradually relaxed the demands they made of public companies, once the auditors realized that some of their initial approaches to enforcing the new law were unrealistic and unnecessary.
- **New standards:** The same organization may fall subject to new standards: for example, any publicly-held company founded outside the United States is subject to Sarbanes-Oxley as soon as it starts doing business in the US.
- **Organization-specific rules:** As discussed earlier, organizations want to enforce their own business rules, which may change over time. They may also want to change the behavior of particular features in ways that better fit the corporate culture.

Many of these evolutions require no coding at all, so it may be misleading to lump them all under the rubric of *customization*. However, where coding is involved, the robustness of the API is important, as is the degree to which it is based on standards that developers already know.

The features of the Xythos applications (Digital Locker and Enterprise Document Manager) represent a small fraction of the functionality in the underlying APIs. The application generally follows a version of the 80/20 Rule: provide the 20% of the potential functionality that 80% of the population can use immediately. The applications are, therefore, a good starting point for customization, since they already present functionality that the average, non-technical person can understand and use. Where you take the functionality, is entirely up to you.

Common Customizations

The following table summarizes some of the common customizations that customers and partners have made to our system to address specific compliance requirements.

CUSTOMIZING XYTHOS FOR COMPLIANCE			
Customization	Description	Compliance usage	Xythos specifics
Digital signatures (workflows)	Add a non-disputable electronic signature (copy of a physical signature, encryption key, etc.) to a workflow approval, rejection, or other action.	Verify that the head researchers approved the protocols for a drug development project.	The customization links these non-disputable signatures from their source (for example, a key broker) to specific Xythos features (workflow approvals,

CUSTOMIZING XYTHOS FOR COMPLIANCE			
Customization	Description	Compliance usage	Xythos specifics
			document check-in, comments on documents, etc.).
Digital signing	Force the user to log in again before taking some action, such as a workflow approval. Acts as a check against the user leaving an application running and unattended.	Ensures that, at the moment the CFO approved the quarterly earnings report for release, that specific person was logged into the system.	A customization can force the user to re-authenticate when approving a workflow, checking in a document, or performing some other critical action.
Biometric authentication	The system uses a retinal scan, fingerprint, or other biometric information as an additional authentication criterion.	Biometric authentication demonstrates even more convincingly that the researcher who updated a protocol document was in fact the person authorized to do so.	The LDAP service integrated with Xythos handles the biometric authentication. Only users who have passed this additional level of authentication can then access the Xythos server.
Smartcard authentication	The user has to provide a registered smartcard before logging into the system.	Any Department of Defense records management system enforces the smartcard requirement before letting the user log in.	Again, Xythos lets the LDAP service handle the additional authentication requirement, then in turn grants access to users who have passed this extra level of security.
Encryption (server-side)	The system automatically encrypts files that are stored in particular folders, or anywhere in the system. Users must present a recognized decryption key before they can read these files.	Any documents containing personal information about students is automatically encrypted, helping a college or university address FERPA requirements.	The Xythos server is integrated with an encryption service that handles document encryption and decryption, key brokerage, and related tasks. An event listener detects the upload of a document into a special folder, the application of a particular document class, or other action that triggers automatic encryption.
Packaged delivery	Users identify a collection of related documents, and then package them for delivery and publication.	Lawyers find the content required for an electronic discovery, collect this information, and add any documentation. The lawyers then pass along this package to the courts or other lawyers as required in the discovery order.	A customized web UI lets users tag documents included in discovery as they browse and search. Optionally, tagged documents include a comment that explains why they were included in the discovery. When finished, the complete package is included in a ZIP file or a folder, which is then shared through a ticket.
Workflow (business process management)	The system presents a library of business processes that detail how users should handle particular kinds of	This electronic library of policies and procedures is easily available to a Sarbanes-Oxley auditor looking for a company's	Using the workflow engine embedded in the Xythos WebFile Server, a developer builds custom workflow

CUSTOMIZING XYTHOS FOR COMPLIANCE			
Customization	Description	Compliance usage	Xythos specifics
	content (for example, approving a vacation request).	documentation of internal financial controls.	screens that display any business processes the organization wants to electronically model and track.
Workflow-triggered actions	The completion of a workflow triggers some action (move, delete, change security, version, etc.) in the system.	Whenever a Freedom of Information Act (FOIA) request gets its final approval, the electronic documents in question are automatically copied to a folder, where they are shared with the people who requested them.	A completed workflow triggers copy, move, version, and other actions in Xythos. The system automatically sends notification to the interested parties, perhaps granting access through a ticket.
Central metadata repository	The organization develops a central library of metadata, which it then applies to documents, email, ERP data, and other forms of electronic information.	The standard set of HIPAA codes for medical conditions can be applied to any content, including documents.	The central metadata repository uses some interface (XML documents, direct calls to the Java API, etc.) to define the metadata available in Xythos.

Putting It All Together

Xythos and Sarbanes-Oxley

OVERVIEW

The portion of the Sarbanes-Oxley Act that has created some of the greatest anxiety is Section 404, which mandates that companies demonstrate the breadth and depth of their internal controls on finances. The Section 404 requirements are designed to prevent the accounting shenanigans that led to the Worldcom, Enron, and Tyco scandals. While the authors of the Sarbanes-Oxley Act assumed that companies would have little trouble collecting the proof of internal controls, in practice, the task of collecting this information for federal auditors proved far harder than expected.

Needless to say, collecting all the relevant documentation for the yearly audit proved to be as challenging as dealing with the auditors themselves. With experience and time, some aspects of Sarbanes-Oxley audits have grown easier to handle. However, as long as users store documents on their own laptop or desktop computers, departmental file servers, and other systems, or forward them to each other as email attachments, the Section 404 requirements will continue to be a huge chore. The cost of failure—various federal penalties, ranging from fines to restrictions on the company's ability to trade stock or do business at all—remain the same.

COLLECTING, SHARING, AND REVIEWING INTERNAL CONTROLS

While shared understandings of Sarbanes-Oxley are growing, there is no single blueprint for Sarbanes-Oxley compliance that every organization can apply to every IT system. The critical question, *Are internal controls sufficient?*, does not mandate that companies organize and manage all forms of electronic information in exactly the same way, using the same tools. Here, then, is a possible starting point for Sarbanes-Oxley compliance, using Xythos products.

For example, the Chief Financial Officer (CFO) mandates that all policy and procedures manuals will be stored in a particular directory on Xythos. All content that goes into this folder will automatically be versioned, and there will be a record of all users who have viewed or edited the file. It is therefore possible for the CFO, when needed, to demonstrate what the policies and procedures manuals said at a particular point in time, and all the users who accessed those versions of the manuals. The CFO also sets the expiration on these manuals to

six months, so that there will be a regular reminder to review and update accounting policies. By using Xythos' workflow features, the CFO also maintains a record of the individuals who approved changes to the company's internal financial controls. Once the new draft is completed, the CFO locks it to further change until the next review period.

The CFO also mandates that all email and instant messaging traffic related to internal controls be stored in a special subfolder for later reference. These steps alone eliminate one of the biggest hurdles towards meeting the Section 404 requirements: rather than hunting down all the relevant internal controls documents, the information is already stored in one place. As an extra precaution, the CFO does regular searches on the content of documents, to make sure that relevant information isn't accidentally left out of the initial presentation to the auditors. If the CFO runs this kind of search regularly, Xythos can save it, making it possible to re-run the search at any time with a single click.

Next, the CFO applies some of Xythos' features to implement these internal controls. Operational documents, such as budget spreadsheets and contracts, need to be strictly controlled. According to Sarbanes-Oxley guidelines, the accounts receivable group should not have access to accounts payable documents. Membership in these groups is already defined in the company's LDAP service, so there is no need to create and maintain a duplicate membership list in Xythos. In this fashion, the CFO creates AR and AP directories that allow these two groups to see each other's documents, if needed, but not alter them. The CFO can therefore demonstrate that the company is not able to play the sort of accounting shell games that led to the collapse of Enron. This security works whether users are uploading documents to these directories, or the ERP system is outputting financial data as spreadsheets or other types of documents. (Xythos can look like a mapped drive equally to applications and human beings.)

Later, the Finance department needs to demonstrate these internal controls to government auditors. The CFO can copy the internal control documents to a staging directory for the auditors, or even share them in place through a ticket. The staging directory may be the better approach, however, if for no other reason than it provides a shared workspace for the auditors to upload their required changes to policies and procedures. The Finance department can use the same workspace for documenting the company's official response to the auditors.

FEATURES USED

In this example, the Xythos features used to address Sarbanes-Oxley requirements include:

- ACL-based security
- Tickets
- Versioning
- Logging
- Expiration
- Workflow
- Desktop access
- Content-based search
- Saved search
- Locking
- LDAP integration

Xythos and HIPAA

OVERVIEW

In the world of day-to-day collaboration and BCS, the important HIPAA requirements are privacy and accessibility. Individuals need assurance that their medical information remains private. At the same time, they need access to their own medical information, and they need to authorize distributing pieces of it to health care providers and insurance companies, as needed. While in the physical world, this balance between privacy and accessibility may be perfectly understandable, in the electronic world, it poses a tricky balancing act. The Internet

has expanded our expectations of information availability; spyware, adware, viruses, worms, and hackers have all exploited that availability.

HIPAA AND HUMAN SUBJECTS

A concrete example best illustrates how Xythos can address these demanding requirements. Private information about a "human subject" in a drug trial clearly falls under HIPAA guidelines. (In fact, the protection of private information was already part of drug development: research protocols demanded the removal of all identifying information from human subject data.) The basic features of Xythos will help protect private information, track who has accessed this information, make it easy to distribute data, scrubbed of identifying information, make all relevant information available to the patient, and classify the patient's condition according to HIPAA condition codes.

For a fictional drug trial, the company has created a home directory for each human subject. The only people with access to a home directory are the patient and the human subject administrator. Using a standard Microsoft Word template, the patient fills out a weekly or monthly self-report, describing the effects of the experimental drug. The patient uploads the latest self-report through the desktop, using the Xythos Drive, or through the web UI. Both mechanisms use a secure HTTP connection, so there is no significant risk of someone intercepting the self-report during upload. If the drug trial participants want to be extra careful, they might also use a desktop utility to encrypt these documents—as long as the subject administrator has the key to decrypt them.

If the subject administrator wants the user to add identifying information to the document itself, such as the period covered in the report, the batch of the experimental drug used, or the full list of conditions the patient is suffering, this information can be added via a document class and custom metadata when the patient uploads the report through the web UI. Versioning and logging are turned on by default in the user's home directory, so from this point forward, the system maintains a complete record of all activity on the new self-report.

The subject administrator now needs to respond. The patient can start a workflow, alerting the subject administrator that the self-report is now available. Alternately, the subject administrator may have a subscription on the home folder, in which case the system sends an email alert that the new self-report is now available. The subject administrator reviews the document, and perhaps tells the patient that some critical information is missing. The missing information may be *in* the document (content), or it may be *on* the document (metadata). As soon as the document is deemed ready, the administrator can approve any workflow the patient started, and then begin the process of scrubbing the document of identifying information.

The subject administrator creates a copy of the self-report in the same directory as the original. In Microsoft Word, the administrator removes any identifying information about the patient. The system continues to version and log changes to the document, which maintains an electronic paper trail on both the scrubbed and raw copies of the self-report. When finished, the subject administrator sets a flag on the document (another custom attribute) indicating that the scrubbed version is complete. The administrator applies a retention rule, which automatically handles two important tasks:

1. The system knows how long the document should be retained (or archived permanently).
2. The system applies a permissions template, sharing the scrubbed version with the research staff.

At this point, researchers have a number of ways they can access the document. The subject administrator may send a researcher a notification email containing an Intellilink (a URL that will work, even if someone later moves or renames it) to the scrubbed version of the self-report. The researchers themselves may have saved searches that they regularly run to see the list of all self-reports filed within a particular period, all self-reports that filed for a

particular batch of the experimental drug, or all cases where the human subjects reported a particular side-effect (which may be captured as one of the HIPAA condition codes).

Later, the human subject can access his own self-reports. The logs provide a history of who has viewed or edited these documents. In other words, the system already documents exactly how private his personal information has remained.

FEATURES USED

The following Xythos features were used in this HIPAA example include the following:

- Secure upload through the Xythos Drive and web UI
- Categorization through a document class
- Extra information about a document, added as custom metadata
- Workflow
- Versioning
- Logging
- Retention rules
- Permission templates
- Intellilink
- Saved searches

Conclusion

Building an effective collaboration and BCS foundation is critical for transforming compliance projects from a burden into an investment. The needs of the individual, the organization, and outside agencies can all be met with the same BCS features, so compliance may turn into a reason to address a host of other needs, including enhanced manageability, improved efficiency and reduced corporate risk.

This document is not the final word on how Xythos' products can be used to address a specific compliance standard, as each organization is different. For further information on how we may address the compliance requirements facing you, contact Xythos at info@xythos.com.