THINKstrategies

A White Paper for Business Decision Makers

Cost-Effective Document Management Solutions for Business-Critical Processes – Part III

Guidelines for Choosing an Online Workspace Provider for Critical Information Exchange

An Independent Perspective Sponsored by:

INTRALINKS

Introduction

The business environment is experiencing rapid changes that are driving companies of all sizes to reevaluate how they exchange information and ideas in a safe and cost-effective manner.

Globalization and mobility are creating more dispersed workplaces, and making it more difficult for employees to communicate with one another or with a host of external parties on a face-to-face basis. Instead, most organizations rely on an assortment of physical and electronic communications methods to transmit important documents and corporate information inside and outside their offices.

Yet, businesses that must share highly proprietary information across their organizations or with outside firms are becoming increasingly aware of the security and compliance risks associated with these activities. While they would like to implement more rigorous security and compliance measures to offset these risks, they also want to streamline their business processes to encourage greater internal collaboration and better external communication as well.

Therefore, organizations of all sizes and especially those that rely on sensitive document-centric processes are seeking a new approach to critical information exchange. This approach is particularly important for processes such as:

- Financial transactions (acquisitions, divestitures, loan and lease syndication, real estate sales, capital raising, etc.)
- Regulatory compliance and audit processes
- Alliance, partnership, joint venture and licensing management
- RFP and large-scale project management
- Investor reporting and board of directors communication

This is Part III of a white paper series that has examined the business demands driving the growth of a new type of enterprise content management solution delivered in a Software-as-a-Service (SaaS) model called an ***online workspace for critical information exchange***.

Part I of this series explores the limitations of traditional approaches to business-critical information sharing and provides an overview of online workspaces as an alternative to the current document management methods. Part II defines the SaaS delivery model for enterprise content management (ECM), describes the business benefits of online workspaces, and provides examples of how these workspaces support critical information exchange for document-intensive processes.

This paper provides guidelines for IT and business decision-makers seeking a document management and exchange solution to support business-critical processes. The guidelines will help decision-makers evaluate online workspace providers for critical information exchange.

What's Driving Businesses to Search for a New Method to Support Critical Information Exchange?

Businesses of all sizes must communicate more effectively with a wide network of external parties to gain and maintain a competitive edge in a rapidly changing marketplace.

In addition to having to create effective internal communications systems to coordinate the efforts of an increasingly dispersed workforce, businesses must also implement mechanisms to communicate with their customers, suppliers, advisors, investors and others to ensure their success. This communication often entails transmitting high volumes of sensitive information to people outside an organization who do not have access to the corporate network.

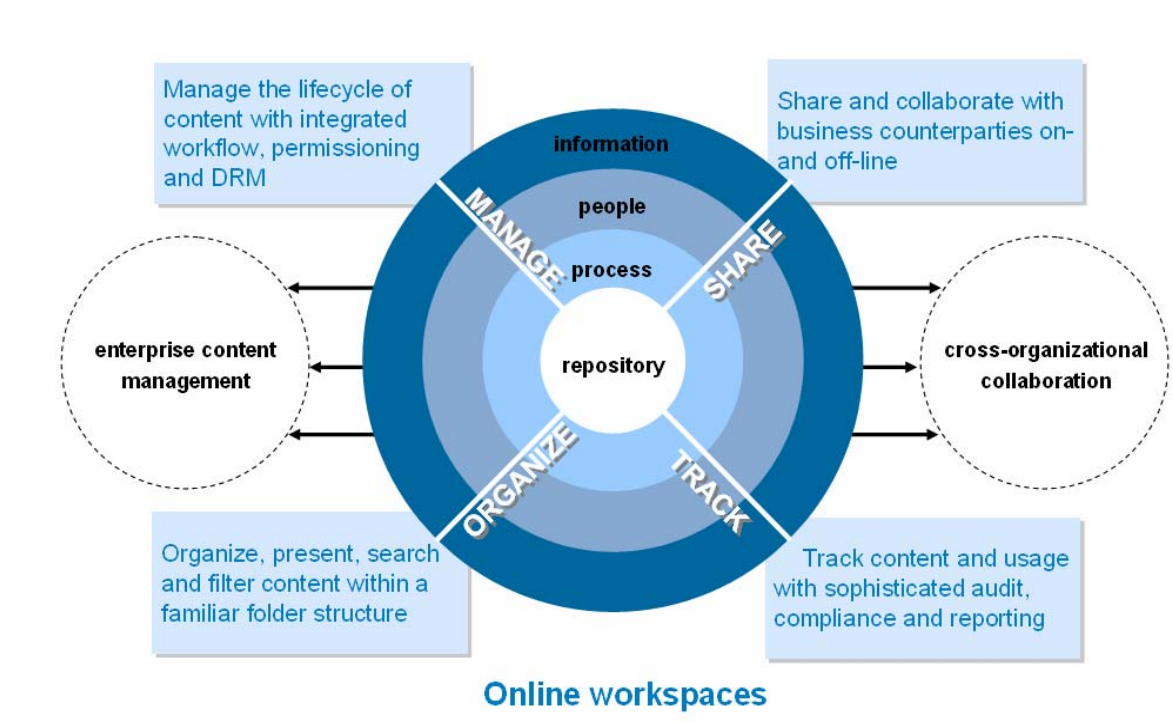
Finding a secure, compliant and cost-efficient means of exchanging highly sensitive information is becoming an increasingly urgent issue as a result of changing workplace dynamics, regulatory requirements and economic conditions.

Online Workspaces for Critical Information Exchange

Online workspaces are a document management solution delivered in a web-based, Software-as-a-Service (SaaS) model.

Online workspaces enable organizations to securely exchange the business-critical and sensitive documents that support essential business processes. They allow companies to grant access to users inside and outside the company firewall—from anywhere, at anytime—more easily. The online workspace, or critical information exchange, also enables organizations to track, organize and manage documents.

Figure 1
Online Workspaces for Critical Information Exchange



There are a wide range of business processes that require the exchange of large volumes of sensitive information with external partners and internal teams.

Common applications for online workspace solutions include:

- Financial transactions (acquisitions, divestitures, loan and lease syndication, real estate sales, capital raising, etc.)
- Regulatory compliance and audit processes
- Alliance, partnership, joint venture and licensing management
- RFP and large-scale project management
- Investor reporting and board of directors communication

Online workspaces are emerging as a more secure, compliant and cost-effective alternative to traditional document exchange methods such as email, fax, overnight mail and FTP, as well as document management solutions deployed on-premise.

Guidelines for Choosing an Online Workspace Provider for Critical Information Exchange

There are two main dimensions on which solution providers should be evaluated.

First is SaaS delivery. Since SaaS is an out-tasking model, it is important to verify a provider can deliver the level of service and capabilities your company requires.

Second is the functionality provided to support online workspaces for critical information exchange. Here you want to be confident the service will meet the document management and exchange demands of your users and will support the security, compliance and cost considerations of your business.

Six Questions for Evaluating SaaS Solutions

1. Is the service reliable?

The first order of business is to determine if the solution meets your organization's requirements for system uptime and availability. Carefully examining performance records to ensure the provider delivers reliable and universal access to valuable documents is a good place to start.

Many providers offer or will negotiate service level agreements (SLAs) that clearly state their availability and performance, identify how these service levels will be monitored and verified, and specify how the provider will be penalized if they fail to meet their obligations.

Disaster recovery and system backup are another key consideration. The provider's servers should be housed in geographically remote, highly secure data centers. The data centers should use real-time replication, multiple connections, alternate power sources and state-of-the-art emergency response systems to ensure data protection.

Note that SLAs should not only state the availability and performance standards to be met, but also the backup and recovery plans, in addition to the problem notification and escalation steps that will be taken if an issue arises.

2. Is the service secure?

There are three key security criteria to review with potential providers to ensure the security of the service infrastructure and business processes.

Infrastructure Security

Disaster recovery, discussed above, is one key aspect of infrastructure security. In addition, the data centers' firewall mechanisms, virus scanning and intrusion detection software should be continuously monitored to assure they are not compromised. It is important to verify that potential providers perform annual tests and audits of their security infrastructure.

Process Security

Process security adds another layer of protection, and is particularly important when SaaS solutions will support highly sensitive company information. It is absolutely critical to ensure that potential providers have thorough security procedures and controls in place to govern every aspect of how client information is managed. Security policies and procedures should be verified using recognized industry standards, such as SAS 70 Type II certification for the financial industry or the FDA's 21 CFR 11 regulations for the life sciences industry.

Personnel Security

Finally, the solution provider's process to ensuring that employees are screened and equipped to handle client's information with the highest integrity and according to strict processes should also be verified. Employees should have thorough background checks. They should undergo intensive training and be required to pass rigorous certification exams. They should also be given ongoing certification training and remain subject to retesting to ensure their skills are up-to-date. And they should be expected to adhere to stringent confidentiality agreements.

Additional security and information protection features specific to document management and control are discussed in the next section on online workspaces for critical information exchange.

3. Is the solution scalable?

For many companies, one reason to consider a SaaS solution is the ability to "pay as you go". Therefore, it makes sense to verify that you can cost-effectively start with a departmental solution and easily add users with the same high levels of security and reliability, as your business demands. The best vendors will be able to add users seamlessly.

4. Can I get my data back easily if I terminate my contact?

Because SaaS business models almost always necessitate housing data with the provider, understanding the process to bring the information back in-house, and ensuring it will not be overly complex and burdensome, is essential.

5. Can I achieve a fast ROI?

Two main drivers for any business case are the financial investments and staff resources required to undertake a program.

Because SaaS solutions do not require a large capital outlay or an investment in staff to maintain the solution, they naturally support a faster ROI than software purchase and implementation.

However, SaaS solutions will require support for implementation. Scoping the effort necessary to implement a solution and train users is part of the smart manager's ROI calculation for executing a new SaaS program.

Evaluate vendors on their support for a turnkey implementation approach, including their ability to upload your company information and integrate with current systems and training.

It is equally important to look at the tools and capabilities vendors provide for you to support and control the implementation at your own pace, should you choose.

Vendors that provide robust service options and strong self-service implementation tools allow maximum control over the implementation process and the cost.

6. Does the solution meet my "must-have" functionality requirements?

It's well known that one of the trade-offs of a SaaS solution is that users may not be able to fully customize the application. This trade-off must be weighed against the significant up-front and ongoing costs of a "build your own", customized solution.

One way to make the calculation is to apply the 80/20 rule to the SaaS solution options. Will the SaaS solution provide 80% of the functionality critical to meeting your business needs, at a substantially lower cost than an on-premise software solution? Can the SaaS solution be configured to meet your needs today, and is the vendor willing and able to work with you to add additional functionality over time?

Additional Questions for Online Workspace Providers

Once a potential provider has been vetted against the SaaS selection criteria, evaluating the provider against online workspaces' specific criteria is the next step. How vendors support critical information exchange should be a primary focus in your evaluation.

1. Will cross-company document exchange and management be made flexible and easy, once and for all?

By definition, online workspaces for critical information exchange are designed to support secure and easy exchange of sensitive information inside and outside your company. You should evaluate several aspects of the service to gauge the relative flexibility and ease of one vendor's solution versus another's. Then seek the solution that is easy for the business users and administrators, as well as the IT team. Evaluate solutions on the following dimensions:

- **Ease of getting documents uploaded and organized**. Are tools available to support bulk load and easy organization of high volumes of documents? Is implementation and use of the tools easy for business users to manage and the IT team to administer?

- **Ease of adoption and use of the service**. Is the interface intuitive? Will the user with an average level of savvy be able to get started on the system with little or no training? This is critical for services that will be used widely across an organization and among external parties. A user-friendly interface correlates directly to wider, faster adoption with less burden on your business and IT managers to facilitate training.
- **Ease of adding new users and administering the system**. Is it required to engage IT to add new users, or can business managers have the flexibility to quickly and easily undertake this task? A main frustration for both groups can be the bottlenecks that occur when IT is required to be the gatekeeper, especially when it is not necessary. Look for providers who can delegate administration to business managers where that option is preferred.
- **24x7xGlobal Dedicated Customer Service**. Does the provider offer comprehensive and responsive global customer service? The ability to support users inside and outside your company around the globe, without putting added burden on your IT staff, adds tremendous value in today's 24x7xglobal business environment.

2. Can I absolutely trust that my critical information will be protected?

The first step to ensuring your data is protected is verifying that your provider meets the reliability and security guidelines outlined earlier. Online workspace providers for critical information exchange should support additional application security capabilities that add significant protection to your sensitive information. Here are the features you should seek:

The Ability to Assign Access Levels and Roles

Solutions should employ a hierarchical role-based system, in which only certain parties are permitted to perform particular functions, such as adding users or posting documents. When users are assigned a role, it determines their overall level of access to documents, and which participants they are able to see within the workspace.

Document Permission

Look for a powerful permissioning system that governs access to each document in your workspace. When a document is posted, those doing the posting should be allowed to determine which users are permitted to see or update it. Users should be able to access the document only as long as those permissions remain in place. Workspace managers should have the capability to change permissions—revoking or adding access for individuals or entire groups— at any time.

Watermarks

To mitigate the risk that someone might print and disseminate sensitive documents, ensure the solution allows you to protect the most important documents in the most commonly used formats with watermarking. This adds an indelible digital fingerprint to the document — and can include the user's name and the date the document was viewed or printed.

Document Locking & Protection

The level of document locking and protection functionality available varies widely across solutions. The strongest document-level protection available uses a powerful security technology that provides the ability to lock down PDF documents.

With this type of solution, the workspace administrator can control whether users can save or print a document, and can even block use of the "print screen" key from taking screenshots. This encryption and locking functionality can be built into every Microsoft Office file-type and PDF document posted — whether it stays in the workspace or is saved to a user's desktop PC. If needed, users can be kept from accessing a document by simply revoking their access, removing them from the workspace or closing the workspace entirely. Confidential information is further protected with 128-bit encryption, one of the highest commercially available encryption levels. Without the proper user ID, password, permission and encryption key, the data is meaningless.

Additional Security Options

To prevent password sharing, the more secure solutions can also prevent a single-user ID from logging in from multiple locations at the same time. And in cases where the strictest security is required, you should ask if your provider can limit a user's access to a single computer.

3. Can the provider demonstrate experience and instill trust?

Another important consideration is the full scope of experience your solution provider has with critical information exchange.

- How long has the company been in business?
- Which company's trust this provider with their critical information today?
- Does the provider have a solid track record of handling highly sensitive information from a wide range of business processes and industries?
- Is the company SAS 70 Type II certified?
- Is the company 21CFR Part II capable?[1]

Answers to these questions will provide a comprehensive profile with which to gauge the experience of the solution provider and help you determine if you can absolutely trust that your critical information will be protected.

4. Will the solution add value and efficiency to my business process?

Improving the efficiency and effectiveness of cross-company collaboration and document exchange are critical to business success today.

Online workspace solutions can help break through the productivity barrier, and add an extra level of information protection to document exchange.

[1] SAS 70 Type II certification in the financial services industry's auditing standard for client data protection. 21CFR Part II is the set of FDA rules for electronic record keeping for clinical drug trials. Providers that meet these criteria by definition have set the bar very high for data protection

Online workspaces have demonstrated 30% reduction in business critical information exchange costs and a 20% improvement in work group productivity.

Online workspace vendors continue to innovate and add features and functionality that further enhance productivity. Here are a few features to look for:

Mobile Access - With more employees and partners working away from the office, the ability to allow system users to access and control documents from mobile devices is a tremendous value-add.

Comprehensive Question and Answer Capability – This workflow capability is particularly important for processes such as due diligence, regulatory management and RFPs where Q&A is central to the process itself. An automated function removes the inefficiencies of spreadsheets and adds an audit trail to the process.

Records and Tracking for Compliance – For processes that require tracking and record keeping for compliance purposes, workspaces are ideal. Look for providers that offer full tracking functionality and provide physical records (DVDs) for closed workspaces. This way you have a permanent record of who accessed which documents, when and for how long. Be sure your solution can ensure compliance now and in the future.

Summary and Conclusion

Businesses are facing escalating competition and becoming more reliant on an increasingly dispersed population of workers, customers and business partners.

In response, they need to transmit and exchange sensitive documents and data internally and externally in a more secure and cost-effective fashion to satisfy the needs of each of these constituencies.

Companies are recognizing that traditional document exchange and collaboration tools are not properly designed to address today's business needs for security, compliance and cost.

Fax and overnight mail are slow and inefficient, and lack sufficient security protections and tracking mechanisms. Email and FTP file transfers are difficult to control and track, and cannot be organized and stored effectively.

Traditional, on-premise document management software applications have proven to be too cumbersome to implement and costly to maintain. They require a significant up-front investment in software licenses, hardware systems and staff. They also entail long deployment cycles and numerous risks that can lead to project failures or cost overruns. And if they are fully deployed, they require dedicated staff to keep them up and running on an ongoing basis.

Most importantly, these on-premise document management applications are not designed to support remote workers or external partners in a consistent and cost-effective fashion, given today's escalating regulations and security concerns.

As a result, a growing number of companies are adopting SaaS online workspaces for critical information exchange to meet their document management needs. This solution can be acquired on a "pay-as-you-go" basis and deployed quickly.

However, IT and business decision-makers must carefully evaluate providers to ensure they have the proper availability, performance, scalability and security measures in place to fully support their corporate requirements.

In addition, a careful review of how online workspace functionality meets their requirements for critical information exchange — including information protection, compliance, ease of use and administration, and efficiency — is recommended.

Business leaders and IT managers in need of secure, compliant, cost-effective document exchange solutions will be well-served to assess online workspaces for their critical information exchange.

This White Paper Was Sponsored by IntraLinks

About IntraLinks

IntraLinks® On-Demand Workspaces™ connect business communities and accelerate the intelligent flow of information and documents among participants. Through IntraLinks' secure, online environments, companies are better able to compete globally by accelerating essential business processes, simplifying communication and fostering rapid workflow.

Since 1997, more than 750,000 participants have used IntraLinks On-Demand Workspaces to communicate and collaborate on over 55,000 projects and transactions in 200 countries. IntraLinks has over 5,000 clients from a wide range of industries. Founded in 1996, IntraLinks is headquartered in New York with offices around the world. For more information, visit www.intralinks.com.

.

About THINKstrategies, Inc.

THINKstrategies is a strategic consulting services company formed specifically to address the unprecedented business challenges facing IT managers, solutions providers and investors today as the technology industry shifts toward a services orientation. The company's mission is to help our clients re-THINK their corporate strategies, and refocus their limited resources to achieve their business objectives. THINKstrategies has also founded the ***Software-as-a-Service Showplace*** *(www.saas-showplace.com), an easy-to-use, online directory and resource center of SaaS solutions organized into over 80 Application, Industry and Enabling Technology categories. The Showplace also includes information and insights regarding industry best practices. For more information regarding our unique services, visit www.thinkstrategies.com, or contact us at info@thinkstrategies.com.*